

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-242039
 (43)Date of publication of application : 29.08.2003

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(51)Int.Cl. G06F 12/14
 G06F 3/06
 G06F 12/00

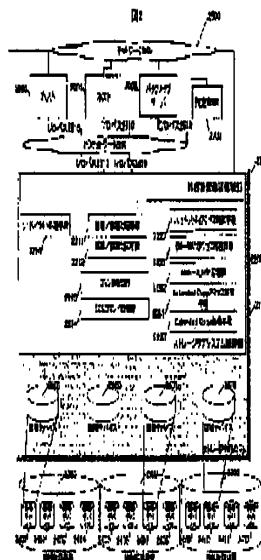
(21)Application number : 2002-043421 (71)Applicant : HITACHI LTD
 (22)Date of filing : 20.02.2002 (72)Inventor : EGUCHI KENTETSU
 ARAKAWA TAKASHI
 FUJITA TAKAHIRO
 TAMURA KEIJI
 OKAMI YOSHINORI

(54) STORAGE SUBSYSTEM, STORAGE CONTROL DEVICE, AND DATA COPY METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent any unauthorized data copy by selectively limiting accesses to a storage subsystem and a storage area in the storage subsystem from the upper rank position.

SOLUTION: When performing the active data copy by a logical storage unit without any computer, acceptance/rejection of the access to the logical storage unit from the computer is checked by the correspondence of WWN of the computer to a logical device identifier LUN, and acceptance/rejection of the access control to each of a copy origin logical storage unit and a copy destination logical storage unit is determined. Unauthorized data outflow by an active copy instruction command from the inside of the storage subsystem can be prevented thereby.



LEGAL STATUS

[Date of request for examination] 30.07.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3993773

[Date of registration] 03.08.2007

[Number of appeal against examiner's decision of rejection]

* NOTICES *

JPO and INPI are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.

2. *** shows the word which can not be translated.

3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] Two or more logic storage which connects with 1 or two or more computers, and said computer makes an I/O object, In the storage subsystem which has a means to process the active data copy directions by said logic store through said calculating machine The storage subsystem characterized by having a means to judge access propriety to the copy data based on the directions from said calculating machine in the case of the active data copy processing by said logic store by the directions from said calculating machine.

[Claim 2] Two or more logic storage which connects with 1 or two or more computers, and said computer makes an I/O object, In the storage subsystem equipped with the port with the fiber channel interface which receives I/O from said calculating machine, and a processing means to control said logic store based on said I/O A maintenance means to hold the access propriety table which associated a discernment means to identify the port of said computer or a computer, and the specific storage region in said logic storage, and defined the access propriety to said storage region from said computer, The association table which associated the address identifier which identifies the port which transmits said discernment means and frame in the communication link demand to a storage subsystem from said calculating machine, A decision means to deduce said discernment means from this association table and said address identifier, and to judge access propriety of said computer from this discernment means and said access propriety table, In the case of active data copy processing of said logic store by directions of said calculating machine The storage subsystem characterized by judging the propriety of access by said calculating machine from said discernment means and said access propriety table using said decision means to the copy data of said calculating machine, and controlling said data copy processing.

[Claim 3] The memory control unit characterized by to have a means judge access propriety to the copy data based on the directions from said computer in the case of the active data copy processing by said logic store by the directions from said computer in two or more logic stores which a computer makes an I/O object, a means process the active data copy directions by said logic store through said computer, and the memory control unit which it has.

[Claim 4] The port in which a computer has two or more logic stores made into an I/O object, and the fiber channel interface which receives I/O from said computer, In the memory control unit equipped with a processing means to control said logic storage based on said I/O A maintenance means to hold the access propriety table which associated a discernment means to identify the port of said computer or a computer, and the specific storage region in said logic storage, and defined the access propriety to said storage region from said computer, The association table which associated the address identifier which identifies the port which transmits said discernment means and frame in the communication link demand to a memory control unit from said computer, A decision means to deduce said discernment means from this association table and said address identifier, and to judge access propriety of said computer from this discernment means and said access propriety table, In the case of active data copy processing of said logic store by directions of said calculating machine The memory control unit characterized by judging the propriety of access by said calculating machine from said discernment means and said access propriety table using said decision means to the copy data of said calculating machine, and controlling said data copy processing.

[Claim 5] The data copy approach characterized by judging access propriety to the copy data based on the directions from said calculating machine through said calculating machine in the data copy approach by the logic store of processing an active data copy, in the case of the active data copy processing by the logic store through a calculating machine.

[Claim 6] the data copy approach which characterizes by to perform the check of a copied material logic store and a copy place logic store which is alike, respectively, receives and judges the propriety of an access control in case the active copy directive command which checks the access propriety to said logic store from a calculating machine through a calculating machine with the correspondence relation between WWN of a calculating machine and a logical device identifier LUN in the data copy approach by the logic store of processing an active data copy, and is published from a calculating machine processes.

[Claim 7] The data copy approach characterized by judging access propriety to the copy data based on the directions from said calculating machine through said calculating machine in the case of the active data copy processing by said logical unit in the data copy approach of performing active copy-of-data processing by the logical unit through a calculating machine.

[Claim 8] The data copy approach characterized by to judge the access propriety to each of a copied material logical unit and a copy place logical unit in case the active data copy directive command which checks the access propriety to said logical unit with the correspondence relation between WWN of a calculating machine and LUN of a logical unit from said calculating machine, and is published from said calculating machine in the data copy approach of performing active copy-of-data processing by the logical unit through a calculating machine is processed.

[Translation done.]

* NOTICES *

JP0 and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] A storage subsystem, a memory control unit, and the data copy approach are started, and this invention is ANSI especially. It is related with the storage subsystem, memory control unit, and the data copy approach of having the fiber channel protocol standardized by X3T11 as an interface with high order equipment.

[0002]

[Description of the Prior Art] ANSI The fiber channel protocol standardized by X3T11 can connect much equipments, and it also has the property in which reservation of security becomes difficult in connection with it about the protocol of varieties, such as SCSI, ESCON (trademark), and TCP/IP, although it has the advantage which can be applied to coincidence.

[0003] First, the description of a fiber channel is explained. A fiber channel is a protocol with the serial transmittal mode without an original commands set, and in order to send information to asynchronous, it has the special feature which can use the bandwidth of a transmission medium effectively. And the fiber channel makes possible more a high speed and variegated data transfer, inheriting the conventional software property by using the physical transmittal mode for instead of [without an original commands set] as a haulageway of commands sets, such as the conventional SCSI and ESCON (trademark).

[0004] A fiber channel is an interface having the description of both channel and network. That is, a fiber channel can perform high-speed data transfer with little delay, once the source and the destination are decided. This is the description of a channel. Moreover, by participating in the communication system of a fiber channel by the opportunity of arbitration, and exchanging information for the device of the partner who becomes the communicative purpose, and mutual, the device which wishes to communicate can recognize each other and can start a communication link. This is the network description. The procedure of information interchange with a partner's device explained here is especially called a log in.

[0005] The part which hits a node, a call, and an actual interface in a device with the interface of a fiber channel is called a port. A node can have one or more ports. The number of the ports which can participate in the whole system of a fiber channel at coincidence is the number of the 24-bit addresses, i.e., about 16,770,000 pieces, at the maximum. The hardware which carries this connection is called a fabric. Since a transmitting agency and the port of a transmission place should just operate only in consideration of the information about a mutual port, without being conscious of a fabric, they argue about a fabric as a logical medium in many cases.

[0006] The unique identifier is memorized all over the world assigned by the fixed Ruhr from a standardization organization in each node and a port. This identifier is equivalent to the MAC Address of TCP/IP, it is the address [**** / in hardware], and calls this address WWN (WORLD WIDE NAME), and has 8 bytes of field.

[0007] The communication link of a fiber channel is Ordered Set. It is performed by the information on the signal level called, and information with a format of the immobilization called a frame.

[0008] A frame consists of 4 bytes of identifier called EOF (EndOf Frame) which shows the end of 4 bytes of identifier called SOF (Start Of Frame) which shows the beginning of a frame, 24 bytes of frame header which performs control of link motion, and characterization of a frame, the data field

which is a part for data division used as the purpose actually transmitted, 4 bytes of cyclic redundancy code (CRC), and a frame. A data field is adjustable in 0-2112 bytes.

[0009] S_ID which is 3 bytes of address identifier for a frame header to identify a transmitting agency port to D_ID and the word [1st] field [23 - 0-bit] which are 3 bytes of address identifier for identifying the transmission place port of a frame to the word [0th] field [23-0-bit] is described, and these identifiers have an effective value with all the frames transmitted and received.

[0010] Address identifier S_ID which identifies a transmitting agency port to a field is a value changed dynamically, and is a value reported from high order equipment, and it depends on the node of the transmitting origin of a frame, WWN of a port, etc. for the value which the fabric is to assign at the time of initialization procedure, and is assigned in FC_CH.

[0011] 8 bytes of field from the head of the data field following a frame header to 21st byte - the 28th byte stores WWN of the port of a transmitting agency, and the frame transmitted from a transmitting agency at the time of a log in stores WWN of the node of transmitting [8 bytes of field from a head to 29th byte - the 36th byte] origin. The equipment of the demand place which received the frame concerned transmits the frame called LS_RJT to log in demand origin, when transmitting the ACC frame to log in demand origin when taking out the information included in this frame and accepting a log in, and refusing a log in.

[0012] If the response of the ACC frame to the frame which oneself transmitted is received, log in demand origin gets to know that the log in was successful, and will be in the condition that I/O processes, such as data transfer, can be started. Moreover, since a log in was not materialized when LS_RJT was received, log in demand origin becomes improper [the I/O process to a log in demand place].

[0013] Although the above-mentioned explained the log in of a class 3, also in other log ins, it is same that WWN and S_ID of a port and a node are contained in the information which can be passed to a log in demand place from log in demand origin.

[0014] As a conventional technique about the approach of preventing unlawful access to a storage subsystem, the technique indicated by JP,10-333839,A, JP,2000-276406,A, etc. is known.

[0015] The approach using the fiber channel protocol as an approach of preventing unlawful access to a storage subsystem is indicated by JP,10-333839,A. This approach is related with WWN (WORLD WIDE NAME) which identifies statically the fiber channel interface (it is called a port) of high order equipments, such as a host computer linked to a storage subsystem, uniquely. Before starting said high order equipment beforehand, WWN of high order equipments, such as said host computer, is made to memorize in a storage subsystem. And the particular port in WWN and a storage subsystem concerned (WWN), Or the table which associates N_Port_Name and the storage region of the arbitration inside a storage subsystem is held. The interior of the frame information published in case the high order equipment concerned accesses a storage subsystem is judged in detail for every frame in a storage subsystem after high order equipment starting the case where permit access when N_Port_Name stored in the frame exists in a table, and it does not exist -- LS_RJT -- by sending out the frame of the connection refusal to say to a high order Access from high order equipment with N_Port_Name which does not exist in said table is refused.

[0016] moreover, to JP,2000-276406,A In above-mentioned JP,10-333839,A, since it is necessary to judge connection propriety for every frame, the communication link engine performance is restricted sharply. Since high order equipment is required to store WWN in all the frames sent out from grade equipment a top when the object of access propriety is the subregion in not a port but a storage subsystem, The technique which solves the technical problem that it is difficult to apply to an actual product from forcing a high order equipment side mounting of the specification outside the standard fiber channel protocol range is indicated.

[0017] WWN which is a discernment means to identify statically uniquely the port of high order equipments, such as a host computer with which this technique accesses a storage subsystem, or high order equipment, Or the table which matched the node name (WWN) of high order equipment and each storage region which is the object of the access propriety judging in a storage subsystem is held in a storage subsystem. furthermore, in case high order equipment communicates with a storage subsystem with WWN of a port or a node using a fiber channel interface, as a means to identify the port of high order equipment or high order equipment uniquely The table which

associated S_ID which is the information dynamically assigned by the login process before informational transmission and reception is held in a storage subsystem. The information acquisition demand to the storage region in a storage subsystem from high order equipment by the opportunity performed using the Inquiry command. The propriety of access to a storage region is judged by using S_ID contained in a demand frame, and searching and comparing said table.

[0018] On the other hand, high order equipment may perform setup/control of storage subsystems, such as a remote copy of a storage region, and a snap shot dump, using control command other than the usual read/write command. The standardization of SAN is performed in SNIA (Storage Networking Industry Association) which is the economic organization which consisted of vendors which treat a SAN (Storage Area Network) product regardless of hardware, software, etc. At the backup subcommittee of SNIA, the standardization of SCSI EXTENDED COPY is performed as a SCSI escape protocol of a SAN application, and two or more vendors are due to use the common specifications standardized here. SCSI EXTENDED COPY is a common protocol for performing the communication link between the equipment which enables server less backup which does not mind a host computer, in order to back up the data in storage in the host computer and storage which were connected with the fiber channel protocol by SAN etc.

[0019]

[Problem(s) to be Solved by the Invention] Drawing 1 is drawing showing the relation between a storage subsystem and a host computer, and explains the trouble of the conventional technique using this drawing.

[0020] In drawing 1, the host computer connected to the storage subsystem 1100 and the storage subsystem 1100 is considered. Here, the host computers connected to the storage subsystem 1100 shall be a host computer A1030, a host computer B1020, and the backup server C1010, and the backup server C1010 shall have the function to back up the data in the storage subsystem 1100 to a tape unit 1210 using snap shot dump 1300 grade (1600). moreover, in the storage subsystem 1100 It is supposed that there are logic storage device LU_A1110, LU_B1120, and LU_C1130. A host computer A1030, a host computer B1020, and the backup server C1010 By the check of Means WWN (World Wide Name) which identifies uniquely the port of the fiber channel of high order equipments, such as a host computer explained in the column of the conventional technique =?

<6//&N0001=522&N0552=9&N0553=000003" TARGET="tjtemdrw" drawing 1 As shown in (a), it shall be set up so that each of the calculating machine which is high order equipment cannot access logic storage device LU_A1110 in the storage subsystem 1100, LU_B1120, and LU_C1130 (access permission 1400). Moreover, LU_C1130 shall be the volume for taking the replication (static image) at the time of there being LU_A1110.

[0021] In the above-mentioned, now, host computer A performs an I/O process between LU_A, host computer B performs an I/O process between LU_B, and the backup server C presupposes that it is backing up by making the data in LU_C applicable to backup along with the schedule which the user set up. In this case, when access is tried from a host computer B1020 to logical device LU_A in the storage subsystem 1100 concerned, or LU_C, WWN of a host computer B1020 is checked and access (log in) has come to be unable to do a host computer B1020 to said logical device LU_A1110 or LU_C1130 in the storage subsystem 1100 in the case of the conventional technique (1500).

[0022] However, as shown in drawing 1 (b), host computer B is said SCSIEXTENDED here. A COPY command is used. Said SCSI EXTENDED A COPY command is published to accessible LU_B1120. The storage subsystem exterior where the contents of the command can access the high order equipment concerned from logical device LU_C1130 which host computer B which published the command concerned originally cannot access. For example, when it is a copy to tape unit 1220 grade, a check is not given to the outflow of storing-in said logical device LU_A1110 or LU_C1130 data. Consequently, unjust access to the data in the storage region which originally cannot be accessed is attained.

[0023] As mentioned above, the conventional technique has the trouble that unjust access to the data in the storage region which originally cannot be accessed is attained.

[0024] The purpose of this invention solves the trouble of the conventional technique mentioned above, and is SCSI EXTENDED. It is in offering the storage subsystem which can prevent an unjust data copy, a memory control unit, and the data copy approach by realizing the security check in the

WWN level in copied material volume, and restricting alternatively access to the storage region in a storage subsystem and a storage subsystem from two or more high order equipments to the data copy from the storage subsystem by control command, such as a COPY command.

[0025]

[Means for Solving the Problem] Two or more logic storage which said purpose is connected to 1 or two or more computers according to this invention, and said computer makes an I/O object, In the storage subsystem equipped with the port with the fiber channel interface which receives I/O from said calculating machine, and a processing means to control said logic store based on said I/O A maintenance means to hold the access propriety table which associated a discernment means to identify the port of said computer or a computer, and the specific storage region in said logic storage, and defined the access propriety to said storage region from said computer, The association table which associated the address identifier which identifies the port which transmits said discernment means and frame in the communication link demand to a storage subsystem from said calculating machine, A decision means to deduce said discernment means from this association table and said address identifier, and to judge access propriety of said computer from this discernment means and said access propriety table, In the case of active data copy processing of said logic store by directions of said calculating machine The propriety of access by said calculating machine is judged from said discernment means and said access propriety table using said decision means to the copy data of said calculating machine, and it is attained by controlling said data copy processing.

[0026]

[Embodiment of the Invention] Hereafter, a drawing explains the operation gestalt of the tray JISABU system by this invention, a memory control unit, and the data copy approach to a detail. In addition, this invention is not limited by the operation gestalt.

[0027] Drawing 2 is the block diagram showing the configuration of the computer system using the storage subsystem by 1 operation gestalt of this invention. In drawing 2 a host computer 2002 2000 and 2001 A backup server, A storage subsystem and 2200 2100 A storage subsystem control section (memory control unit), A read/write processing means, and 2211 and 2212 2210 The information corresponding to logic/physics, 2213 the SCSI command-processing section and 2220 for the command-processing section and 2214 A LUN security access-control means, LUN-WWN access propriety information and 2222 2221 The information corresponding to WWN-S_ID, 2230 is EXTENDED COPY. A processing means and 2231 are EXTENDED COPY. Access-control means, 2240 -- the external device communications processing section and 2300 — physical memory equipment and 2401- for a logical device and 2500, as for an I/O network and 2610, a network and 2600 are [2412 and 2420 / an I/O bus and 2700] setting terminals.

[0028] The computer system shown in drawing 2 is constituted by host computers 2000 and 2001, the backup server 2002, the storage subsystem 2100, and the setting terminal 2700, and host computers 2000 and 2001, the backup server 2002 and the storage subsystem 2100, and the control terminal 2700 are connected by the network 2500. As a network 2500, you may be Ethernet (trademark), FDDI, a fiber channel, a public line network, etc., and a control terminal is usually used for the maintenance control working-level month of a storage subsystem, for example.

[0029] Moreover, it connects with the storage subsystem 2100 through the I/O network 2600 and I/O bus 2610, and host computers 2000 and 2001 and the backup server 2002 emit the lead of data, and I/O for light processing to the storage subsystem 2100. In case host computers 2000 and 2001 and the backup server 2002 publish I/O, they are usually accessed through the address of a logical storage region to the data in the storage subsystem 2100. As the I/O network 2600 and I/O bus 2610, many means, such as a fiber channel, SCSI, ESCON (trademark), Ethernet (trademark), and Infiniband (trademark), can be used, for example.

[0030] The external communications processing section 2240 of the storage subsystem 2100 is performed, when communications processing with external devices, such as a host, a backup server, and a setting terminal, is combined with communication link transmission lines, such as a fiber channel, SCSI, ESCON (trademark), and Ethernet (trademark), a protocol, etc. and a suitable interface offers it.

[0031] In addition, two and a backup server do not need to be limited for a host computer as showed equipment connectable with the illustration storage subsystem 2100 in drawing to one etc.,

and at least one or more calculating machines may usually be connected to one or more storage subsystems.

[0032] By the way, as for this invention, a certain device which received the command from a host computer aims at establishing a security device in storage equipment about performing a copy etc. to other devices which are different from this from other devices again through the host computer. [0033] It is SCSI EXTENDED COPY Command as what is supporting current and such a command. Since it is, explanation of the operation gestalt of subsequent this inventions is continued by making this command into an example. Moreover, the I/O bus which connects a host computer and a storage subsystem shall perform communications control in connection with transmission and reception of a SCSI command, and continues explanation of the operation gestalt of this invention by making a fiber channel into an example as one of them here.

[0034] Now, the storage subsystem 2100 consists of a storage subsystem control section 2200 and two or more physical memory equipments 2300. usually, the host computer which packs two or more physical memory equipments, constitutes a disk array in order that a mass storage subsystem may maintain the safety and the dependability of a system, builds a logical storage region on it, and is connected to a storage subsystem — receiving — other logical devices — logical device 2401- it provides as 2412 and 2420.

[0035] The storage subsystem control section 2200 receives physical memory equipment 2300. The information 2211 corresponding to a logic storage region / physical memory field is referred to for the read/write processing demand from a host computer. Carry out logic / physical correspondence with the means 2212 corresponding to logic/physics, and the read/write means 2210 performs read/write processing to a suitable storage region, and also The demand from various host computers is processed, or it is processing offering information required for maintenance/management of storage subsystems, such as the operation information and fault information of a storage subsystem, and management information, to the setting terminal 2700 or a host computer etc.

[0036] Moreover, the storage subsystem control section 2200 It connects with the storage subsystem 2100. The correspondence relation information 2221 and the host computer of access propriety of LUN which are the identifier of 2412 and 2420 mind a fiber channel. logical device 2400- in coming WWN of a host computer, and the storage subsystem 2100 — the correspondence relation information 2222 on S_ID in the fiber channel frame transmitted in case it connects, and WWN of a host computer — and Based on the correspondence relation information 2221 on the access propriety of said LUN, S_ID, and the correspondence relation information 2222 on WWN of a host computer, it has a LUN security access-control means 2220 to perform a LUN access control.

[0037] Furthermore, the storage subsystem control section 2200 is SCSI EXTENDED COPY Command to a specific logical device. EXTENDED COPY Command which interprets the command when it receives, and performs suitable processing The processing means 2230 and its EXTENDED COPY Command EXTENDED COPY which prevents the outflow of inaccurate data It has the access-control means 2231. In addition, even if it has the storage region mapped by the physical storage region, it is not necessary to have the logical device. Moreover, there may be more than one in a storage subsystem in itself [storage subsystem control-section].

[0038] Moreover, although it also holds information [such as configuration information in a storage subsystem,] required in order to process respectively as a system, such as access operation information over a logic store or a cache, a parity group's configuration information, and its RAID level information, since the storage subsystem control section 2200 is not important in explanation of the operation gestalt of this invention, it omits those explanation here. In addition, in order to carry out processing which comes out, respectively to a host computer, a backup server, said above-mentioned storage subsystem control section, and an above-mentioned setting terminal, the component which surely exists in computers, such as memory for storing a program and information, CPU, and an internal data communication way, also exists in them, respectively, but in explanation of the operation gestalt of this invention, since it is not important, those explanation is omitted here.

[0039] Next, drawing indicated by Information technology—SCSI Primary Command -3 (SPC3) currently indicated as a draft of a SCSI commands set by t10 Technical Committee is used, and it

is SCSI EXTENDED. About a format of a COPY command, the copy from a block device to a streams device etc. is explained as an example.

[0040] Drawing 3 is EXTENDED COPY Command. It is drawing explaining the configuration of Command Descriptor Block (CDB).

[0041] EXTENDED COPY Command The process code 3100 which CDB consists of 16 bytes and is indicated by the cutting tool 0 is 83h (it is shown that h is a hexadecimal display). A cutting tool 14 is a reserve field with a cutting tool 1 to the cutting tool 9, and it is EXTENDED COPY Command even to the cutting tool 13 from a cutting tool 10. Die-length PARAMETER LIST LENGTH 3200 of a parameter list is indicated.

[0042] EXTENDED COPY Command A parameter required for activation is indicated and transmitted to a data out buffer from a host computer to a storage subsystem besides assignment by CDB in the data out phase which transmits the data specified from the initiator in SCSI by the command to the target following CDB.

[0043] In addition, when the value of above-mentioned PARAMETER LIST LENGTH 3200 is 0, it is shown that no data were transmitted and it is not an error.

[0044] Drawing 4 is drawing explaining the configuration of EXTENDED COPY Command PARAMETER List. Drawing 3 explained this list — as — the process code of CDB — 83h — it is — EXTENDED COPY Command it is — ** — EXTENDED COPY Command indicated in the data out buffer when distinguished It is a format of a command parameter list required for activation, and PARAMETER LIST LENGTH 3200 shown in Drawing 3 shows the die length of this parameter list with a byte value.

[0045] EXTENDED COPY Command A parameter list consists of the header unit 4700 which consists of 16 bytes, a target descriptor 4500 which continues after that, a segment descriptor 4600, and in-line data as an option. A header unit 4700 consists of each data of LIST IDENTIFIER4100, STR, NRCR, a command priority, the die length 4200 of a target descriptor list, the die length 4300 of a segment descriptor list, and the die length 4400 of in-line data.

[0046] A cutting tool's 0 LIST IDENTIFIER4100 is SCSI EXTENDED COPY Command by client application. It is the value chosen in order to decide uniquely to a copy manager. 7 which looks like [a cutting tool 1] and can be set, and the 6 or 3rd bit are reserve, and PRIORITY is written in NRCR and the 2-0th bit at the 5th bit at STR and the 4th bit.

[0047] The die length of the target descriptor 4500 which is the target descriptor length 4200 and is indicated from a cutting tool 16 is indicated by cutting tools 2 and 3, it is reserve, cutting tools 8-11 are segment descriptor length (4300), and cutting tools 4-7 have indicated a segment descriptor's 4600 die length indicated from a cutting tool n+1. In addition, n is the byte count of the last the target descriptor in this parameter list is indicated to be.

[0048] Drawing 5 is drawing explaining the detail of the contents of the target descriptor 4500 from the cutting tool 16 in the command parameter list shown in Drawing 4 to a cutting tool n. It is described by 32 bytes per one and this target descriptor is EXTENDED COPY Command. The data about a copied material or a copy place are described.

[0049] The descriptor type code 5100 is described by the cutting tool 0 of an illustration target descriptor, and it is Fiber Channel World Wide Name. In the case of a target descriptor, the code is E0h. The device type 5200 is described by the cutting tool 1. Moreover, Logical Unit Number(LUN) 5300 of a target is described even from a cutting tool 4 to a cutting tool 11, and World Wide Name (WWN) 5400 of a target is described by even cutting tools 12-19. Furthermore, a cutting tool 28 to the cutting tool 31 is Device Type Specific Parameter 5500, and the parameter of the device type proper of a target is described.

[0050] Drawing 6 is drawing explaining an example of the detailed contents of the parameter 5500 of the device proper described by the cutting tool 31 from the cutting tool 28 of the target descriptor shown in Drawing 5, and is a format in case the device type specified by a cutting tool's 1 bit 4-0 is a block device (for example, disk) in a target descriptor.

[0051] Drawing 7 is drawing explaining other examples of the detailed contents of the parameter 5500 of the device proper described by the cutting tool 31 from the cutting tool 28 of the target descriptor shown in Drawing 5, and is a format when the device type specified by a cutting tool's 1 bit 4-0 is a sequential access device (for example, tape) in a target descriptor.

[0052] Drawing 8 is drawing explaining the example of the one detailed contents of the segment

descriptor 4600 described by cutting tool $n+m$ from the cutting tool $n+1$ in the command parameter list shown in drawing 4. In addition, m is a data length the segment descriptor is indicated to be by the parameter list.

[0053] The cutting tool 0 of an illustration target descriptor is Descriptor Type Code8100, and if it is a copy from a block device to a sequential access device, or a copy from a sequential access device to a block device, which code of 00h, 01h, 0Bh, and 0Ch will be described here. The remainder 8800 bit length of the segment descriptor which continues after the descriptor length 8200 is indicated and this descriptor length is indicated is described by cutting tools 2 and 3. In the copy to a tape device from the above-mentioned block device, the code described here is 14h.

[0054] The source target descriptor index 8300 which becomes a copied material is described by cutting tools 4 and 5, and the destination target descriptor index 8400 of a copy place is described by cutting tools 6 and 7. These indexes correspond to drawing 4 with the index of the target descriptor 4500 in the command parameter list of a publication. Cutting tools 9-11 are the streams device transfer length 8500, and have specified the amount which writes data in a streams device. Moreover, cutting tools 14 and 15 are 8600 block device blocks, and correspond with DISK BLOCK LENGTH 6100 described in the format of the target descriptor of drawing 5. BLOCK

DEVICELOGICAL BLOCK ADDRESS (LBA)8700 described by cutting tools 16-23 is the logic block address of the beginning on Block Device.

[0055] EXTENDED COPY Command shown in drawing 3 explained by the above-mentioned - drawing 8 The related format is indicated as a draft of a SCSI commands set in t10 Technical Committee. For this reason, the contents of the format mentioned above only illustrated that the information which can specify copied material copy places, such as WWN of a target and LUN, was included in the above-mentioned format in the above-mentioned although it may change from now on, and are EXTENDED COPY Command fundamentally. It is not influenced by modification of a detail part.

[0056] Next, EXTENDED COPY Command The access control to access to the inaccurate device to twist is explained.

[0057] EXTENDED COPY Command mentioned above In the case of a fiber channel, it is dedicated to a fiber channel frame and transmitted to a storage subsystem from high order equipment. Then, a fiber channel frame is explained first.

[0058] Drawing 9 is drawing explaining the configuration of the frame of a fiber channel. An illustration frame consists of 4 bytes of identifier called 4 bytes of identifier called SOF (start of frame)9000 which shows the beginning of a frame, 24 bytes of frame header 9100 which performs control of link motion, and characterization of a frame, the cyclic redundancy code (CRC) 9300 of 9200 or 5 bytes of data field which is a part for the data division used as the purpose actually transmitted, and EOF (end of frame)9400 which shows the end of a frame. A data field is adjustable among 0-2112 bytes.

[0059] Drawing 10 is drawing explaining the configuration of the frame header unit 9100 in the frame of the fiber channel mentioned above.

[0060] The frame header unit 9100 is constituted by six WORD with each bit, and the 23-0-bit field of D_ID (Distination ID)10100 and WORD1 of the 23-0-bit field of WORD0 is S_ID (Source ID)10200. S_ID10200 is 3 bytes of address identifier for identifying the port which transmits this fiber channel frame, and D_ID10100 is 3 bytes of address identifier which identifies the port which receives this fiber channel frame. Both identifiers have an effective value with all the frames transmitted and received. S_ID10200 is the information which can identify dynamically high order equipments (a host computer, backup server, etc.) uniquely, the device of the transmitting origin which sends a fiber channel frame in a fiber channel, and the device of a transmission place are the values reported to each other from high order equipment at the time of the log in which exchanges information mutually, and when establishing a logic session between devices, it is used.

[0061] By using a fiber channel frame which was mentioned above, a host computer, a backup server, etc. become possible [performing an I/O process through a storage subsystem and a fiber channel].

[0062] Next, in this invention, a fiber channel network is minded from high order equipment (a host computer and backup server), and it is SCSI EXTENDED. The example of the information table which the storage subsystem for receiving a fiber channel frame with a COPY command has is

explained.

[0063] Drawing 11 is drawing explaining the example of the table which performs matching with S_ID in the fiber channel frame transmitted to a storage subsystem from high order equipment (for example, host computer), and WWN of the high order equipment corresponding to it.

[0064] An illustration table is created by acquiring WWN and S_ID of a host computer (port of a host computer bus adapter) from a fiber channel frame etc. in case a host computer logs in to a storage subsystem through a fiber channel.

[0065] The usual fiber channel communicates after a log in using S_ID and D_ID. Eye 11100 1 of the table shown in drawing 11 train is in S_ID, and eye 11200 two trains is WWN of the host computer corresponding to it.

[0066] The storage subsystem which received the fiber channel frame can take out S_ID in a fiber channel frame, and can acquire WWN corresponding to S_ID which searched and matched eye 1 of an illustration table train. Thereby, WWN of a host computer which has transmitted the fiber channel frame can be specified.

[0067] In addition, since log in processing of a fiber channel is not directly related to this invention, explanation here is omitted.

[0068] That is, a host computer is EXTENDED COPY Command to the logical device of the storage subsystem after a fiber channel log in. When it transmits, the storage subsystem control section 2200 which controls the logical device which receives the command is ** which can deduce WWN of a host computer which has transmitted the frame corresponding to the S_ID with reference to the table which takes out S_ID from a fiber channel frame header, and is shown in drawing 11.

[0069] Drawing 12 is drawing explaining the example of the LUN-WWN access propriety information 2221 shown in drawing 2, and the example which showed the correspondence relation whether the host computer which has a certain WWN in LUN12000 associated for every port of the port (WWN:1234567890ABCDEF of a port) 12000 with WWN12100 and the storage subsystem of a host computer could access at which LUN is illustrated as a table.

[0070] In the case of the operation gestalt of this invention currently explained, the table shown in drawing 12 is created for every port on a storage subsystem, and the plurality for several port minutes which exists in a storage subsystem exists. And creation of a table is performed from a storage subsystem and the equipment 2700 for maintenance which can be communicated, for example, a setting terminal, by directing using the display means for checking an input means and its input result.

[0071] Although it is common to be carried out as a setting means from the setting terminal for maintenance of the storage subsystem connected to the storage subsystem by LAN, the telephone line, or the internal bus, the location of the configurator which, as for this invention, sets them up, the class of those setting means and setting terminal, especially the class of network to be used, etc. are not asked. Moreover, WWN used here presupposes that it is known.

[0072] If LAN is used and a setup from the location near a storage subsystem and the telephone line will be used according to the class of communication line, a maintenance center etc. can be set up from a remote place. Moreover, it is possible to also make the equipment for maintenance and a storage subsystem unify using an internal bus.

[0073] LUN shows LU related with the port and only the number of the host computers which may access the number of WWN(s) to LU which exists in the port subordinate exists. The number of LU and host computers turns into a limited number.

[0074] In each element of a table, with the operation gestalt of this invention, a value "1" will mean an access permission and a value "0" will mean access refusal.

[0075] In the case of the example shown in drawing 12, in the port, the host computer which has an access permission to LUN0 (12210) is a host computer in which WWN has "0123456789ABCDEF" and "0123456789ABCDE", and the host computer which has an access permission to LUN1 (12220) is a host computer in which WWN has "0123456789ABCDEF". Moreover, in the case of the example of illustration, the host computer with which access to LUNn-1 (12230) is permitted means not existing.

[0076] Now, a host computer is EXTENDED COPY Command. If it publishes to the logical device of a storage subsystem, when a storage subsystem receives this command, WWN of a host computer and the identifier LUN of the logical device which is the transmission place of a command are

checked, and after evaluating whether it is accessible, a logical device will receive this command and will begin to analyze the contents of the command. the received command — EXTENDED COPY Command it is — a case — EXTENDED COPY The command receipt logical device serves as a copy manager, and the processing means 2230 is controlled to perform a copy of data to the logical device of a copy place from the logical device of the copy origin indicated in the command. [0077] Drawing 13 is a flow chart explaining the example of processing actuation of renewal of LUN - WNN access propriety information, next explains this. The table which matches S_ID in the fiber channel frame with which the example explained here is transmitted to a storage subsystem from the high order equipment (for example, host computer) explained by drawing 11, and WNN of the high order equipment corresponding to it, In the example of the LUN-WNN access propriety information 2221 on drawing 2 which looked like [drawing 12] and was explained more in LUN with WNN of a host computer, and a storage subsystem associated for every port It is an example of the procedure of the storage subsystem control section about a setup with the table having shown the correspondence relation of to which LUN a host computer with a certain WNN is made as for accesses (port log in etc.). In addition, the case where a logical device is newly in addition to the logical device set up beforehand set up is mentioned as an example, and is explained here.

[0078] (1) first — for example, a host computer and a backup server are the copy place applications to a remote place etc., and newly specified the logical device as the volume connected distantly in the network physically [the volume which are applications such as a disaster recovery as a device for the replication (static image) at the time of there being a logical volume which performs READ/WRITE, and performs a host's I/O process] — direct using the I/O network 2600 or a network 2500 so that it may be vacant and may assign from a physical memory field. Or a storage subsystem manager uses the setting terminal 2700, and directs to assign from the empty physical memory field which newly specified the logical device corresponding to the demand from a host computer user. The storage subsystem control section 2200 receives the demand, and updates the information 2212 corresponding to logic/physics for a logical device using allocation and the means 2211 corresponding to logic/physics from the appointed empty physical memory field (steps 13100 and 13200).

[0079] (2) Next, the storage subsystem control section 2200 updates the LUN-WNN access propriety information 2221 that resembled drawing 12 and it explained more, to the assigned logical device. It is carried out so that it may say that this updating permits WNN of the backup server which issued directions, and WNN of a HOST computer which performs an I/O process for the data which perform backup by the forward volume side to the logical device assigned newly, for example (step 13300).

[0080] A storage subsystem manager may set up the renewal of the LUN-WNN access propriety information 2221 mentioned above using a setting terminal, and the command-processing section 2213 in a storage subsystem control section may perform it by carrying out program manipulation of the LUN SECURITY setting processing, for example.

[0081] Drawing 14 minds a fiber channel network and is SCSI EXTENDED. It is a flow chart explaining the example of processing actuation with the device which received the COPY command, next this is explained. The example explained here minds a fiber channel network from high order equipment, and is SCSI EXTENDED. The storage subsystem control section 2200 which received the fiber channel frame when the COPY command had been transmitted, and EXTENDED COPY The access processing means 2230 and EXTENDED COPY It is the example of the processing which a receipt logical device performs with the access-control means 2231.

[0082] Moreover, it is EXTENDED COPY Command here. The case where it is transmitted to a storage subsystem from a host computer through a fiber channel network as a frame containing the information unit called FCP_CMND shown in drawing 9 is described.

[0083] (1) Check the storage subsystem which receives the fiber channel frame from a host computer as shown in drawing 2 using the table on which S_ID and WNN are taken out from a frame, and the correspondence table of WNN as shown in S_ID and drawing 11 of a host computer of the fiber channel frame transmitting origin is first created in processing of a fiber channel log in, and the host computer concerned shows drawing 12 whether it is accessible to the assignment device in a storage subsystem. Then, a storage subsystem receives the fiber channel frame transmitted from the above-mentioned host computer to an internal specific-logical device (step 14000).

[0084] (2) Reception of a fiber channel frame takes out S_ID in a frame header so that WNN of a host computer which has transmitted this frame can be identified. Next, the data field of a frame is read and the case where Command Device Block (CDB) is in a fiber channel frame estimates whether the contents of the command are EXTENDED COPY Command (steps 14010 and 14020). [0085] (3) the fiber channel frame received by evaluation of step 14020 — EXTENDED COPY Command it was not — a case — others — it shifts to processing (step 14031).

[0086] (4) the fiber channel frame received by evaluation of step 14020 — EXTENDED COPY Command it was — a case, next the parameter length in CDB are evaluated, if parameter length is 0, processing will be ended, and if parameter length is not 0, the read in of the command parameter list following CDB which ~~**4**~~(ed) will be started (step 14030).

[0087] (5) Read cutting tools' 2 and 3 target descriptor length after reading the list ID of [in a command parameter list] etc. here, target descriptor length was TL — it carries out (step 14040). [0088] (6) Next, read cutting tools' 8-11 segment descriptor length. Here, segment descriptor length presupposes that it was SL (step 14050).

[0089] (7) Read the target descriptor 1 target descriptor length part (32Byte) every after reading the in-line data length of a parameter list. In addition, this EXTENDED COPY Command The number of the target descriptors contained is TL/32. Drawing 5 has already explained the format of a target descriptor, and first, it evaluates the type code of a descriptor and reads WNN and LUN of a target. Processing of the read in of the above-mentioned 1 target descriptor is repeated by the target descriptor number (TL / 32 pieces) (steps 14060-14100).

[0090] (8) Next, perform a segment descriptor's read in. Drawing 8 has already explained a segment descriptor's format, and it reads a descriptor type code, descriptor length (DL), etc. first. Next, the descriptor index of the source target used as a copied material logical device and the descriptor index of the destination target used as a copy place logical device are read (steps 14120-14150).

[0091] (9) Read WNN of a source target, and LUN here with reference to the target descriptor shown in drawing 5 by using as a key the target descriptor index described by segment disk PURITA. The table of the access propriety of the host computer WNN and logical device (LU) which are shown in drawing 12 is referred to. WNN and LUN, and this EXTENDED COPY Command of a source target It evaluates whether it is accessible to the logical device with which the host computer of WNN which transmitted was specified as the source target (steps 14160 and 14170).

[0092] (10) By evaluation at step 14170, when accessible, read a segment descriptor's remainder, read transfer length, LBA of the number of block devices, and a block device, etc., and copy the specified data copy towards the logical device specified as the destination target from the logical device specified with the source target (step 14180).

[0093] (11) And repeat the processing from step 14120 in which the next segment descriptor is read. SL/(DL+4) ***** which can be found from said descriptor length (DL) and segment disk PURPUTA length (SL) in this (steps 14110-14190).

[0094] As opposed to the logical device specified as the source target by evaluation at step 14170 (12) Access refusal or when impossible. This EXTENDED COPY Command It ends by CHECK CONDITION status. For example, sense key Set up COPY ABORT, set COPY TARGET DEVICE NOT REACHABLE as sense code, and as exception handling corresponding to this EXTENDED COPY Command Defined suitable error processing is performed, a host is notified of an error, and processing is ended (steps 14210 and 14200).

[0095] In addition, although explained by the above-mentioned having carried out error processing only to the part of access propriety, error processing of the command itself is set for every occasional step of the, and it is EXTENDED COPY Command. There are some which were defined, and it is followed when an error naturally occurs.

[0096] (13) Moreover, if it can check that the processing mentioned above for all segment descriptors at step 14190 has been completed, when an in-line data length will be 0, it is EXTENDED COPY Command. It is processing EXTENDED COPY Command Defined normal termination processing is performed and it is EXTENDED COPY Command. Processing is ended (step 14200).

[0097] Drawing 15 minds a fiber channel network and is SCSI EXTENDED. It is a flow chart explaining other examples of processing actuation with the device which received the COPY command, next this is explained. The example explained here minds a fiber channel network from

high order equipment, and is SCSI EXTENDED. When the COPY command has been transmitted The storage subsystem control section 2200 which received the fiber channel frame, EXTENDED COPY The access processing means 2230 and EXTENDED COPY As opposed to what was controlled by the flow which is the example of the processing which a receipt logical device performs with the access-control means 2231, and is shown in drawing 14 The processing (steps 15170-15190) which also evaluates WWN of a publication and LUN using an access propriety table on a LUN access table to a destination target descriptor is added. To the logical volume which is having processing reserved beforehand a sake [the replication inside a storage subsystem, or for a remote copy], it is specified as a copy place and this added processing is EXTENDED COPY. It can use for the ability not to perform copy processing.

[0098] Here, it is EXTENDED COPY Command. It controls about the case where it is transmitted to a storage subsystem from a host computer through a fiber channel network as a frame containing the information unit called FCP_CMND shown in drawing 9.

[0099] (1) Check the storage subsystem which receives the fiber channel frame from a host computer as shown in drawing 2 using the table on which S_ID and WWN are taken out from a frame, and the correspondence table of WWN as shown in S_ID and drawing 11 of a host computer of the fiber channel frame transmitting origin is first created in processing of a fiber channel log in, and the host computer concerned shows drawing 12 whether it is accessible to the assignment device in a storage subsystem. Then, a storage subsystem receives the fiber channel frame transmitted from the above-mentioned host computer to an internal specific-logical device (step 15000).

[0100] (2) Reception of a fiber channel frame takes out S_ID in a frame header so that WWN of a host computer which has transmitted this frame can be identified. Next, the data field of a frame is read and the case where Command Device Block (CDB) is in a fiber channel frame estimates whether the contents of the command are EXTENDED COPY Command (steps 15010 and 15020).

[0101] (3) the fiber channel frame received by evaluation of step 15020 -- EXTENDED COPY Command it was not -- a case -- others -- it shifts to processing (step 15031).

[0102] (4) the fiber channel frame received by evaluation of step 15020 -- EXTENDED COPY Command it was -- a case, next the parameter length in CDB are evaluated, if parameter length is 0, processing will be ended, and if parameter length is not 0, the read in of the command parameter list following CDB which **4**^{ed} will be started (step 15030).

[0103] (5) Read cutting tools' 2 and 3 target descriptor length after reading the list ID of [in a command parameter list] etc. here, target descriptor length was TL -- it carries out (step 15040).

[0104] (6) Next, read cutting tools' 8-11 segment descriptor length. Here, segment descriptor length presupposes that it was SL (step 15050).

[0105] (7) Read the target descriptor 1 target descriptor length part (32Byte) every after reading the in-line data length of a parameter list. In addition, this EXTENDED COPY Command The number of the target descriptors contained is TL/32. Drawing 5 has already explained the format of a target descriptor, and first, it evaluates the type code of a descriptor and reads WWN and LUN of a target. Processing of the read in of the above-mentioned 1 target descriptor is repeated by the target descriptor number (TL / 32 pieces) (steps 15060-15100).

[0106] (8) Next, perform a segment descriptor's read in. Drawing 8 has already explained a segment descriptor's format, and it reads a descriptor type code, descriptor length (DL), etc. first. Next, the descriptor index of the source target used as a copied material logical device and the descriptor index of the destination target used as a copy place logical device are read (steps 15120-15150).

[0107] (9) Read WWN of a source target, and LUN here with reference to the target descriptor shown in drawing 5 by using as a key the target descriptor index described by segment disk PURITA.

The table of the access propriety of the host computer WWN and logical device (LU) which are shown in drawing 12 is referred to. WWN and LUN, and this EXTENDED COPY Command of a source target It evaluates whether it is accessible to the logical device with which the host computer of WWN which transmitted was specified as the source target (steps 15160 and 15170).

[0108] (10) By evaluation at step 15170, when accessible next, read the descriptor index of the destination target used as the logical device of a copy place, and refer to a target descriptor (step 15180).

[0109] (11) Use as a key the target descriptor index described by segment disk PURITA here. WWN of a destination target and LUN are read with reference to the target descriptor shown in drawing

5 . The table of the access propriety of the host computer WWN and logical device (LU) which are shown in drawing 12 is referred to. WWN and LUN, and this EXTENDED COPY Command of a destination target As opposed to the logical device with which the host computer of WWN which transmitted was specified as the source target It evaluates whether it is accessible (steps 15190 and 15200).

[0110] (12) By evaluation at step 15200, when accessible, read a segment descriptor's remainder, read transfer length, LBA of the number of block devices, and a block device, etc., and copy the specified data copy towards the logical device specified as the destination target from the logical device specified with the source target (step 15210).

[0111] (13) And repeat the processing from step 15120 in which the next segment descriptor is read. SL/(DL+4) ***** which can be found from said descriptor length (DL) and segment disk PURPUTA length (SL) in this (steps 15110-15220).

[0112] By evaluation at steps 15170 and 15200, (14) A source target, As opposed to the logical device specified as the destination target In or when [access refusal or when impossible] This EXTENDED COPY Command It ends by CHECK CONDITION status. For example, sense key Set up COPY ABORT, set COPY TARGET DEVICE NOT REACHABLE as sense code, and as exception handling corresponding to this EXTENDED COPY Command Defined suitable error processing is performed, a host is notified of an error, and processing is ended (steps 15230 and 15240).

[0113] In addition, although explained by the above-mentioned having carried out error processing only to the part of access propriety, error processing of the command itself is set for every occasional step of the, and it is EXTENDED COPY Command. There are some which were defined, and it is followed when an error naturally occurs.

[0114] (15) Moreover, if it can check that the processing mentioned above for all segment descriptors at step 15220 has been completed, when an in-line data length will be 0, it is EXTENDED COPY Command. It is processing EXTENDED COPY Command Defined normal termination processing is performed and it is EXTENDED COPY Command. Processing is ended (step 15240).

[0115] The access propriety information between the devices which memorize the identifier and information on high order equipment according to the operation gestalt of this invention mentioned above, By having an access propriety judging means using the information maintenance and its information, and a means to judge the propriety of copy activation at the time of the copy processing activation by the active copy directive command from the interior of a storage subsystem The access propriety to the logical device in a storage subsystem from high order equipments, such as a host computer It adds to checking with the correspondence relation between WWN of high order equipment, and the logical device identifier LUN. In case the active copy directive command from the interior of a storage subsystem published from high order equipment to a storage subsystem is processed It judges, when the copy receipt logical device used as a copy directions device performs the check which performs an access control to a copied material device and the copy place devices of each. The outflow of the inaccurate data based on the active copy directive command from the interior of a storage subsystem can be prevented.

[0116]

[Effect of the Invention] According to [as explained above] this invention, it is SCSI EXTENDED. To the data copy from the storage subsystem by control command, such as a COPY command, the security check in the WWN level in copied material volume can be realized, it can make it possible to restrict alternatively access to the storage region in a storage subsystem and a storage subsystem from two or more high order equipments, and an unjust data copy can be prevented.

[Translation done.]

* NOTICES *

JP0 and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.*** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the relation of the storage subsystem and host computer explaining the trouble of the conventional technique.

[Drawing 2] It is the block diagram showing the configuration of the computer system using the storage subsystem by 1 operation gestalt of this invention.

[Drawing 3] EXTENDED COPY Command It is drawing explaining the configuration of Command Descriptor Block (CDB).

[Drawing 4] It is drawing explaining the configuration of EXTENDED COPY Command PARAMETER List.

[Drawing 5] It is drawing explaining the detail of the contents of the target descriptor 4500 from the cutting tool 16 in the command parameter list shown in drawing 4 to a cutting tool n.

[Drawing 6] It is drawing explaining an example of the detailed contents of the parameter of the device proper described by the cutting tool 31 from the cutting tool 28 of the target descriptor shown in drawing 5.

[Drawing 7] It is drawing explaining other examples of the detailed contents of the parameter of the device proper described by the cutting tool 31 from the cutting tool 28 of the target descriptor shown in drawing 5.

[Drawing 8] It is drawing explaining the example of the segment descriptor's detailed contents described by cutting tool n+m from the cutting tool n+1 in the command parameter list shown in drawing 4.

[Drawing 9] It is drawing explaining the configuration of the frame of a fiber channel.

[Drawing 10] It is drawing explaining the configuration of the frame header unit in the frame of the fiber channel mentioned above.

[Drawing 11] It is drawing explaining the example of the table which performs matching with S_ID in the fiber channel frame transmitted to a storage subsystem from high order equipment, and WWN of the high order equipment corresponding to it.

[Drawing 12] It is drawing explaining the example of the LUN-WWN access propriety information shown in drawing 2.

[Drawing 13] It is a flow chart explaining the example of processing actuation of renewal of LUN-WWN access propriety information.

[Drawing 14] A fiber channel network is minded and it is SCSI EXTENDED. It is a flow chart explaining the example of processing actuation with the device which received the COPY command.

[Drawing 15] A fiber channel network is minded and it is SCSI EXTENDED. It is a flow chart explaining other examples of processing actuation with the device which received the COPY command.

[Description of Notations]

2000 2001 Host computer

2002 Backup Server

2100 Storage Subsystem

2200 Storage Subsystem Control Section

2210 Read/write Processing Means

2211 2212 Information corresponding to logic/physics

2213 Command-Processing Section

2214 SCSI Command-Processing Section

2220 LUN Security Access-Control Means

2221 LUN-WWN Access Propriety Information

2222 Information corresponding to WWN-S_ID

2230 EXTENDED COPY Processing Means

2231 EXTENDED COPY Access-Control Means

2240 External Device Communications Processing Section

2300 Physical Memory Equipment

2401- 2412 and 2420 Logical device

2500 Network

2600 I/O Network

2610 I/O Bus

2700 Setting Terminal

[Translation done.]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-242039

(P2003-242039A)

(43)公開日 平成15年8月29日 (2003.8.29)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 1 7
3/06	3 0 4	3/06	3 0 4 M 5 B 0 6 5
12/00	5 3 1	12/00	5 3 1 M 5 B 0 8 2
	5 3 7		5 3 7 M

審査請求 未請求 請求項の数 8 O.L. (全 16 頁)

(21)出願番号 特願2002-43421(P2002-43421)

(22)出願日 平成14年2月20日 (2002.2.20)

(71)出願人 000005108
 株式会社日立製作所
 東京都千代田区神田駿河台四丁目6番地

(72)発明者 江口 賢哲
 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 荒川 敬史
 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74)代理人 100093492
 弁理士 鈴木 市郎 (外1名)

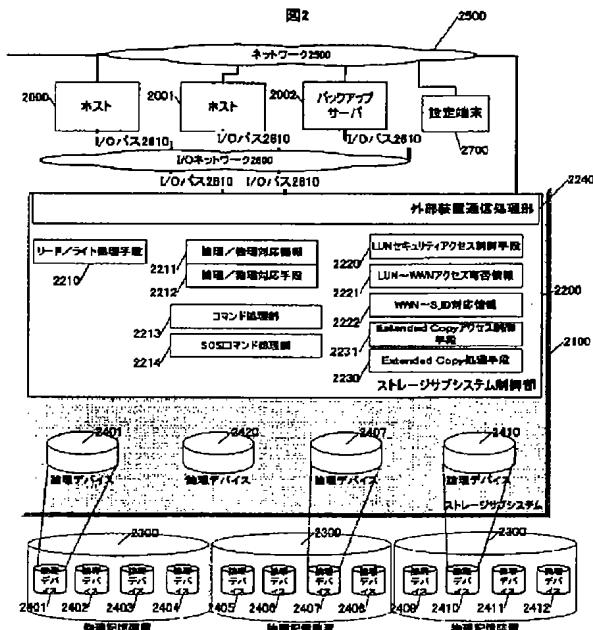
最終頁に統ぐ

(54)【発明の名称】ストレージサブシステム、記憶制御装置及びデータコピー方法

(57)【要約】

【課題】 上位装置からストレージサブシステム及びストレージサブシステム内の記憶領域へのアクセスを選択的に制限し、不正なデータコピーを防止する。

【解決手段】 計算機を介すことなく論理記憶装置による能動的なデータコピーの処理を行う際に、計算機から前記論理記憶装置に対するアクセス可否を計算機のWWNと論理デバイス識別子LUNとの対応関係によりチェックし、コピー元論理記憶装置とコピー先論理記憶装置とのそれぞれに対してアクセス制御の可否を判定する。これにより、ストレージサブシステム内部からの能動的なコピー指示コマンドによる不正なデータの流出を防ぐことができる。



【特許請求の範囲】

【請求項1】 1または複数の計算機に接続され、前記計算機がI/O対象とする複数の論理記憶装置と、前記計算機を介すことなく前記論理記憶装置による能動的なデータコピー指示の処理を行う手段とを有するストレージサブシステムにおいて、前記計算機からの指示による前記論理記憶装置による能動的なデータコピー処理の際に前記計算機からの指示によるコピーデータに対してアクセス可否の判断を行う手段を有することを特徴とするストレージサブシステム。

【請求項2】 1または複数の計算機に接続され、前記計算機がI/O対象とする複数の論理記憶装置と、前記計算機からのI/Oを受信するファイバチャネルインターフェースを持つポートと、前記I/Oに基づき前記論理記憶装置を制御する処理手段とを備えたストレージサブシステムにおいて、前記計算機あるいは計算機のポートを識別する識別手段と前記論理記憶装置内の特定の記憶領域とを関連付け、前記計算機から前記記憶領域に対するアクセス可否を定義したアクセス可否テーブルを保持する保持手段と、前記計算機からストレージサブシステムへの通信要求内の前記識別手段とフレームを送信するポートを識別するアドレス識別子とを関連付けた関連テーブルと、該関連テーブルと前記アドレス識別子とから前記識別手段を割り出し、該識別手段と前記アクセス可否テーブルとから前記計算機のアクセス可否の判断を行う判断手段と、前記計算機の指示による前記論理記憶装置の能動的なデータコピー処理の際に、前記計算機のコピーデータに対して前記識別手段と前記アクセス可否テーブルとから前記計算機によるアクセスの可否を前記判断手段を用いて判定して、前記データコピー処理の制御を行うことを特徴とするストレージサブシステム。

【請求項3】 計算機がI/O対象とする複数の論理記憶装置と、前記計算機を介すことなく前記論理記憶装置による能動的なデータコピー指示の処理を行う手段と有する記憶制御装置において、前記計算機からの指示による前記論理記憶装置による能動的なデータコピー処理の際に前記計算機からの指示によるコピーデータに対してアクセス可否の判断を行う手段を有することを特徴とする記憶制御装置。

【請求項4】 計算機がI/O対象とする複数の論理記憶装置と、前記計算機からのI/Oを受信するファイバチャネルインターフェースを持つポートと、前記I/Oに基づき前記論理記憶装置を制御する処理手段とを備えた記憶制御装置において、前記計算機あるいは計算機のポートを識別する識別手段と前記論理記憶装置内の特定の記憶領域とを関連付け、前記計算機から前記記憶領域に対するアクセス可否を定義したアクセス可否テーブルを保持する保持手段と、前記計算機から記憶制御装置への通信要求内の前記識別手段とフレームを送信するポートを識別するアドレス識別子とを関連付けた関連テーブル

と、該関連テーブルと前記アドレス識別子とから前記識別手段を割り出し、該識別手段と前記アクセス可否テーブルとから前記計算機のアクセス可否の判断を行う判断手段と、前記計算機の指示による前記論理記憶装置の能動的なデータコピー処理の際に、前記計算機のコピーデータに対して前記識別手段と前記アクセス可否テーブルとから前記計算機によるアクセスの可否を前記判断手段を用いて判定して、前記データコピー処理の制御を行うことを特徴とする記憶制御装置。

10 【請求項5】 計算機を介すことなく論理記憶装置による能動的なデータコピーの処理を行うデータコピー方法において、前記計算機を介すことなく論理記憶装置による能動的なデータコピー処理の際に前記計算機からの指示によるコピーデータに対してアクセス可否の判断を行うことを特徴とするデータコピー方法。

【請求項6】 計算機を介すことなく論理記憶装置による能動的なデータコピーの処理を行うデータコピー方法において、計算機から前記論理記憶装置に対するアクセス可否を計算機のWWNと論理デバイス識別子LUNとの対応関係によりチェックし、計算機から発行される能動的なコピー指示コマンドを処理する際に、コピー元論理記憶装置とコピー先論理記憶装置とのそれぞれに対してアクセス制御の可否を判定するチェックを実行することを特徴とするデータコピー方法。

20 【請求項7】 計算機を介すことなく論理装置による能動的なデータのコピー処理を行うデータコピー方法において、前記計算機を介すことなく前記論理装置による能動的なデータコピー処理の際に、前記計算機からの指示によるコピーデータに対するアクセス可否の判断を行うことを特徴とするデータコピー方法。

30 【請求項8】 計算機を介すことなく論理装置による能動的なデータのコピー処理を行うデータコピー方法において、前記計算機から前記論理装置に対するアクセス可否を計算機のWWNと論理装置のLUNとの対応関係によりチェックし、前記計算機から発行される能動的なデータコピー指示コマンドを処理する際に、コピー元論理装置とコピー先論理装置とのそれぞれに対するアクセス可否を判定することを特徴とするデータコピー方法。

【発明の詳細な説明】

40 【0001】

【発明の属する技術分野】 本発明は、ストレージサブシステム、記憶制御装置及びデータコピー方法に係り、特に、ANSI X3T11で標準化されたファイバチャネルプロトコルを、上位装置とのインターフェースとして持つストレージサブシステム、記憶制御装置及びデータコピー方法に関する。

【0002】

【従来の技術】 ANSI X3T11で標準化されたファイバチャネルプロトコルは、多数の装置が接続可能であり、かつ、SCSI、ESCON（登録商標）、TC

P/I P等の多種のプロトコルを同時に運用可能な利点を有するものであるが、それに伴いセキュリティの確保が困難となる性質も併せ持っている。

【0003】まず、ファイバチャネルの特徴について説明する。ファイバチャネルは、独自のコマンドセットを持たないシリアルの転送方式を持つプロトコルであり、情報を非同期に送るために伝送媒体の帯域幅を有効に利用できる特色を持っている。そして、ファイバチャネルは、独自のコマンドセットを持たない代わりに、物理転送方式を、従来のSCSI、ESCON（登録商標）といったコマンドセットの連搬路として使用することにより、従来のソフトウェア資産を継承しながら、より高速かつ多彩なデータ転送を可能としている。

【0004】ファイバチャネルは、チャネルとネットワークとの両者の特徴を併せ持つインターフェースである。すなわち、ファイバチャネルは、一旦転送元と転送先とが確定すれば、遅延が少ない高速なデータ転送を行うことができる。これはチャネルの特徴である。また、通信を希望する機器は、任意の契機でファイバチャネルの通信系に参加し、通信の目的となる相手の機器と相互に情報を交換することにより、互いを認識して通信を開始することができる。これはネットワークの特徴である。ここで説明した相手の機器との情報交換の手続きを、特に、ログインと呼ぶ。

【0005】ファイバチャネルのインターフェースを持つ機器をノードと呼び、実際のインターフェースにあたる部分をポートと呼ぶ。ノードは、1つ以上のポートを持つことが可能である。ファイバチャネルの系全体に同時に参加できるポートの数は、最大で24ビットのアドレスの数、すなわち、約1677万個である。この接続を媒介するハードウェアをファブリックと呼ぶ。送信元及び送信先のポートは、ファブリックを意識せずに互いのポートに関する情報のみを考慮して動作すればよいので、ファブリックを論理的な媒体として議論する場合も多い。

【0006】各ノード及びポートには、標準化団体から一定のルールによって割り当てられる世界中でユニークな識別子が記憶されている。この識別子は、TCP/IPのMACアドレスに相当するものであり、ハードウェア的に固定なアドレスであり、このアドレスをWWN(WORLD WIDE NAME)とよび8バイトの領域を持つ。

【0007】ファイバチャネルの通信は、Ordered Setと呼ばれる信号レベルの情報と、フレームと呼ばれる固定のフォーマットを持った情報とにより行われる。

【0008】フレームは、フレームの始まりを示すSOF(Start Of Frame)と呼ばれる4バイトの識別子、リンク動作の制御やフレームの特徴づけを行う24バイトのフレームヘッダ、実際に転送される目的となるデータ部分であるデータフィールド、4バイトの巡回冗長コード(CRC)、フレームの終わりを示すEOF(End Of

Frame)と呼ばれる4バイトの識別子からなる。データフィールドは、0～2112バイトで可変である。

【0009】フレームヘッダは、0ワード目の23～0ビットの領域に、フレームの送信先ポートを識別するための3バイトのアドレス識別子であるD_ID、1ワード目の23～0ビットの領域に送信元ポートを識別するための3バイトのアドレス識別子であるS_IDが記述してあり、これらの識別子は、送受信される全てのフレームで有効な値を持つ。

【0010】領域に送信元ポートを識別するアドレス識別子S_IDは、動的に変動する値であり上位装置より報告される値であり、FC_CHでは、ファブリックによって初期化手続き時に割り当てられることになっていて、割り当てられる値は、フレームの送信元のノードやポートのWWN等に依存する。

【0011】ログイン時に送信元から送信されるフレームは、フレームヘッダに続くデータフィールドの先頭から21バイト目～28バイト目までの8バイトの領域が送信元のポートのWWNを格納し、先頭から29バイト目～36バイト目までの8バイトの領域が送信元のノードのWWNを格納している。当該フレームを受信した要求先の装置は、このフレームに含まれている情報を取り出し、ログインを受諾する場合、ACCフレームをログイン要求元に対して送信し、ログインを拒絶する場合、LS_RJTと呼ばれるフレームをログイン要求元に対して送信する。

【0012】ログイン要求元は、自らが送信したフレームに対するACCフレームの応答を受信すると、ログインが成功したことを知り、データ転送などのI/Oプロセスを開始できる状態となる。また、ログイン要求元は、LS_RJTを受信した場合、ログインが成立しなかつたため、ログイン要求先へのI/Oプロセスは不可となる。

【0013】前述では、クラス3のログインについて説明したが、他のログインにおいても、ログイン要求元からログイン要求先へ渡すことのできる情報の中に、ポート及びノードのWWNとS_IDが含まれることは同様である。

【0014】ストレージサブシステムに対する不正アクセスを防止する方法に関する従来技術として、例えば、特開平10-333839号公報、特開2000-276406号公報等に記載された技術が知られている。

【0015】特開平10-333839号公報には、ストレージサブシステムに対する不正アクセスを防止する方法として、ファイバチャネルプロトコルを用いた方法が開示されている。この方法は、ストレージサブシステムに接続してくるホスト計算機等の上位装置のファイバチャネルインターフェース(ポートと呼ぶ)を静的に一意に識別するWWN(WORLD WIDE NAME)に関し、予め前記上位装置を起動する前に、ストレージサブシステムの中

に前記ホスト計算機等の上位装置のWWNを記憶させ、かつ、当該WWNとストレージサブシステム中の特定ポート(WWN)、あるいは、N_Port_Nameとストレージサブシステム内部の任意の記憶領域とを関連付けるテーブルを保持し、上位装置起動後、当該上位装置がストレージサブシステムにアクセスする際に発行するフレーム情報の内部を、ストレージサブシステムにおいてフレーム毎に逐一判定して、フレーム内に格納されたN_Port_Nameがテーブル内に存在する場合にアクセスを許可し、存在しない場合、LS_RJTという接続拒否のフレームを上位に対して送出することによって、前記テーブル内に存在しないN_Port_Nameを持つ上位装置からのアクセスを拒否するというものである。

【0016】また、特開2000-276406号公報には、前述の特開平10-333839号公報において、接続可否の判定をフレーム毎に行う必要があるために通信性能が大幅に制限されることと、アクセス可否の対象がポートではなくストレージサブシステム内の部分領域である場合上、位装置から送出されるフレーム全てにWWNを格納することが上位装置に要求されるため、上位装置側に標準ファイバチャネルプロトコル範囲外の仕様の実装を強いることから実際の製品に適用することは困難であること、という課題を解決する技術が開示されている。

【0017】この技術は、ストレージサブシステムにアクセスしてくるホスト計算機等の上位装置あるいは上位装置のポートを静的に一意に識別する識別手段であるWWN、あるいは、上位装置のノード名(WWN)と、ストレージサブシステム内におけるアクセス可否判定の対象である各記憶領域とを対応づけたテーブルとをストレージサブシステム内に保持し、さらに、ポートあるいはノードのWWNと、上位装置がファイバチャネルインターフェースを用いてストレージサブシステムと通信を行う際に、上位装置または上位装置のポートを一意に識別する手段として、情報の送受信に先立つログインプロセスにより動的に割り当てられる情報であるS_IDとを関連付けたテーブルをストレージサブシステム内に保持し、上位装置からストレージサブシステム内の記憶領域に対する情報取得要求が、Inquiryコマンドを用いて行われた契機で、要求フレームに含まれるS_IDを用いて、前記テーブルを検索及び比較することによって記憶領域に対するアクセスの可否を判定するというものである。

【0018】一方、上位装置は、通常のリード/ライトコマンド以外の制御コマンドを用いて、記憶領域のリモートコピーやスナップショット等のストレージサブシステムの設定/制御を行う場合がある。ハードウェア、ソフトウェア等を問わずSAN(Storage Area Network)製品を扱うベンダーで構成された業界団体であるSN

A(Storage Networking Industry Association)では、SANの標準化作業が行われている。SNTAのバックアップ分科会では、SAN用途のSCSI拡張プロトコルとしてSCSI EXTENDED COPYの標準化作業が行われていて、複数のベンダがここで標準化された共通仕様を用いる予定である。SCSI EXTENDED COPYは、SAN等でファイバチャネルプロトコルで接続されたホスト計算機とストレージとにおいて、ストレージ内のデータをバックアップするために、ホスト計算機を介さないサーバレスバックアップを可能とする装置間での通信を行うための共通プロトコルである。

【0019】

【発明が解決しようとする課題】図1はストレージサブシステムとホスト計算機との関係を示す図であり、この図を用いて従来技術の問題点について説明する。

【0020】図1において、ストレージサブシステム1100とストレージサブシステム1100に接続されているホスト計算機について考える。ここでは、ストレージサブシステム1100に接続されているホスト計算機が、ホスト計算機A1030、ホスト計算機B1020、バックアップサーバC1010であり、また、バックアップサーバC1010は、ストレージサブシステム1100内のデータを、スナップショット1300等を使用してテープ装置1210にバックアップ(1600)する機能を持っているものとする。また、ストレージサブシステム1100内には、論理記憶デバイスLU_A1110、LU_B1120、LU_C1130があるとし、ホスト計算機A1030、ホスト計算機B1020とバックアップサーバC1010とは、従来技術の欄で説明したホスト計算機等の上位装置のファイバチャネルのポートを一意に識別する手段WWN(World Wide Name)のチェックにより、図1(a)に示すように、上位装置である計算機のそれぞれがストレージサブシステム1100内の論理記憶デバイスLU_A1110、LU_B1120、LU_C1130にしかアクセスできないように設定されているものとする(アクセス許可1400)。また、LU_C1130は、LU_A1110のある時点のレプリケーション(静的イメージ)をとるためのボリュームになっているものとする。

【0021】前述において、いま、ホスト計算機Aは、LU_Aとの間でI/O処理を行い、ホスト計算機Bは、LU_Bとの間でI/O処理を行い、バックアップサーバCは、LU_Cにあるデータをバックアップ対象として、ユーザが設定したスケジュールに沿って、バックアップを行っているとする。この場合、ホスト計算機B1020から当該ストレージサブシステム1100内の論理デバイスLU_AやLU_Cにアクセスを試みた場合、従来技術の場合、ストレージサブシステム1100において、ホスト計算機B1020のWWNをチェックし、ホスト計算機B1020が前記論理デバイスLU

—A1110やLU_C1130に対してアクセス（ログイン）ができないようになっている（1500）。

【0022】しかし、ここで、図1（b）に示すように、ホスト計算機Bが、前記SCSI EXTENDED COPYコマンドを用い、前記SCSI EXTENDED COPYコマンドをアクセス可能なLU_B1120に発行し、そのコマンドの内容が、当該コマンドを発行したホスト計算機Bが本来アクセスできない論理デバイスLU_C1130から当該上位装置がアクセスできるストレージサブシステム外部の、例えば、テープ装置1220等へのコピーであった場合、前記論理デバイスLU_A1110やLU_C1130内に格納されているデータの流出に対してチェックが施されず、この結果、本来アクセス不可能な記憶領域にあるデータへの不正なアクセスが可能となる。

【0023】前述したように、従来技術は、本来アクセス不可能な記憶領域にあるデータへの不正なアクセスが可能となるという問題点を有している。

【0024】本発明の目的は、前述した従来技術の問題点を解決し、SCSI EXTENDED COPYコマンド等の制御コマンドによるストレージサブシステムからのデータコピーに対し、コピー元ボリュームでのWWNレベルでのセキュリティチェックを実現し、複数の上位装置からストレージサブシステム及びストレージサブシステム内の記憶領域へのアクセスを選択的に制限することにより、不正なデータコピーを防止することのできるストレージサブシステム、記憶制御装置及びデータコピー方法を提供することにある。

【0025】

【課題を解決するための手段】本発明によれば前記目的は、1または複数の計算機に接続され、前記計算機がI/O対象とする複数の論理記憶装置と、前記計算機からのI/Oを受信するファイバチャネルインターフェースを持つポートと、前記I/Oに基づき前記論理記憶装置を制御する処理手段とを備えたストレージサブシステムにおいて、前記計算機あるいは計算機のポートを識別する識別手段と前記論理記憶装置内の特定の記憶領域とを関連付け、前記計算機から前記記憶領域に対するアクセス可否を定義したアクセス可否テーブルを保持する保持手段と、前記計算機からストレージサブシステムへの通信要求内の前記識別手段とフレームを送信するポートを識別するアドレス識別子とを関連付けた関連テーブルと、該関連テーブルと前記アドレス識別子とから前記識別手段を割り出し、該識別手段と前記アクセス可否テーブルとから前記計算機のアクセス可否の判断を行う判断手段と、前記計算機の指示による前記論理記憶装置の能動的なデータコピー処理の際に、前記計算機のコピーデータに対して前記識別手段と前記アクセス可否テーブルとから前記計算機によるアクセスの可否を前記判断手段を用いて判定して、前記データコピー処理の制御を行うこと

により達成される。

【0026】

【発明の実施の形態】以下、本発明によるトレージサブシステム、記憶制御装置及びデータコピー方法の実施形態を図面により詳細に説明する。なお、本発明は、実施形態により限定されるものではない。

【0027】図2は本発明の一実施形態によるストレージサブシステムを用いた計算機システムの構成を示すブロック図である。図2において、2000、2001はホスト計算機、2002はバックアップサーバ、2100はストレージサブシステム、2200はストレージサブシステム制御部（記憶制御装置）、2210はリード/ライト処理手段、2211、2212は論理/物理対応情報、2213はコマンド処理部、2214はSCSIコマンド処理部、2220はLUNセキュリティアクセス制御手段、2221はLUN～WWNアクセス可否情報、2222はWWN～S_ID対応情報、2230はEXTENDED COPY処理手段、2231はEXTENDED COPYアクセス制御手段、2240は外部装置通信処理部、2300は物理記憶装置、2401～2412、2420は論理デバイス、2500はネットワーク、2600はI/Oネットワーク、2610はI/Oバス、2700は設定端末である。

【0028】図2に示す計算機システムは、ホスト計算機2000、2001と、バックアップサーバ2002と、ストレージサブシステム2100と、設定端末2700とにより構成され、ホスト計算機2000、2001及びバックアップサーバ2002とストレージサブシステム2100及び制御端末2700とは、ネットワーク2500により接続されている。ネットワーク2500としては、例えば、イーサネット（登録商標）、FDDI、ファイバチャネル、公衆回線網等であってよく、制御端末は、通常、ストレージサブシステムの保守管理作業用に使用される。

【0029】また、ホスト計算機2000、2001、バックアップサーバ2002は、ストレージサブシステム2100に、I/Oネットワーク2600及びI/Oバス2610を介しても接続され、ストレージサブシステム2100に対してデータのリードやライト処理のためのI/Oを発する。ホスト計算機2000、2001、バックアップサーバ2002は、I/Oを発行する際にストレージサブシステム2100内のデータに対して、通常、論理的な記憶領域のアドレスを通じてアクセスする。I/Oネットワーク2600、I/Oバス2610としては、例えば、ファイバチャネル、SCSI、ESCON（登録商標）、Ethernet（登録商標）、Infiniband（登録商標）等の多くの手段を使用することができる。

【0030】ストレージサブシステム2100の外部通信処理部2240は、ホスト、バックアップサーバ、設

定端末等の外部装置との通信処理を、ファイバチャネル、SCSI、ESCON（登録商標）、Ethernet（登録商標）等の通信伝送路、プロトコル等に併せ適当なインターフェースの提供することにより行う。

【0031】なお、図示ストレージサブシステム2100に接続できる装置は、図に示したようなホスト計算機が2つ、バックアップサーバが1つ等に限定される必要はなく、通常、少なくとも1つ以上の計算機が1つ以上のストレージサブシステムに接続されていてよい。

【0032】ところで本発明は、ホスト計算機からのコマンドを受領した、あるデバイスがホスト計算機を介することなく、他のデバイスからまたこれとは異なる他のデバイスに対してコピーなどを行うことに関して、ストレージ装置においてセキュリティ機構を設けることを目的としている。

【0033】現在、そのようなコマンドをサポートしているものとして、SCSIのEXTENDED COPY Commandがあるので、このコマンドを例として、以降の本発明の実施形態の説明を続ける。また、ホスト計算機とストレージサブシステムとを接続するI/Oバスは、SCSIのコマンドの送受信にかかる通信制御ができるものとし、ここでは、その1つとしてファイバチャネルを例として、本発明の実施形態の説明を続ける。

【0034】さて、ストレージサブシステム2100は、ストレージサブシステム制御部2200及び複数の物理記憶装置2300から構成される。通常、大容量のストレージサブシステムは、システムの安全性・信頼性を保つために複数の物理記憶装置をまとめてディスクアレイを構成し、その上で論理的な記憶領域を構築し、ストレージサブシステムに接続されるホスト計算機に対して、その他の論理的なデバイスと共に、論理デバイス2401～2412、2420として提供している。

【0035】ストレージサブシステム制御部2200は、物理記憶装置2300に対して、ホスト計算機からのリード／ライト処理要求を、論理記憶領域／物理記憶領域対応情報2211を参照し、論理／物理対応手段2212によって論理／物理対応させ、リード／ライト手段2210によって適当な記憶領域に対してリード／ライト処理を行う他、様々なホスト計算機からの要求を処理したり、設定端末2700やホスト計算機に対してストレージサブシステムの稼動情報や障害情報、管理情報等のストレージサブシステムの保守／管理に必要な情報を提供する等の処理を行っている。

【0036】また、ストレージサブシステム制御部2200は、そのストレージサブシステム2100に接続してくるホスト計算機のWWNとストレージサブシステム2100内の論理デバイス2400～2412、2420の識別子であるLUNのアクセス可否の対応関係情報2221やホスト計算機がファイバチャネルを介して接続してくる際に送信してくるファイバチャネルフレーム

内のS_IDとホスト計算機のWWNとの対応関係情報2222、及び、前記LUNのアクセス可否の対応関係情報2221とS_IDとホスト計算機のWWNの対応関係情報2222に基づいて、LUNアクセス制御を行うLUNセキュリティアクセス制御手段2220を持つ。

【0037】さらに、ストレージサブシステム制御部2200は、特定の論理デバイスに対して、SCSIのEXTENDED COPY Commandを受領した際にそのコマンドを解釈し、適当な処理を行うEXTENDED COPY Command処理手段2230と、そのEXTENDED COPY Commandによって、不正なデータの流出を防ぐEXTENDED COPYアクセス制御手段2231を持つ。なお、論理デバイスは、物理的な記憶領域にマッピングされた記憶領域を持っていても、持っていないてもよい。また、ストレージサブシステム制御部それ自体は、ストレージサブシステム内に複数あってもよい。

【0038】また、ストレージサブシステム制御部2200は、論理記憶装置やキャッシュに対してのアクセス稼動情報やパリティグループの構成情報、そのRAIDレベル情報等、ストレージサブシステム内の構成情報等、システムとして各自処理を行うために必要な情報をも保持しているが、本発明の実施形態の説明においては重要ではないので、ここではそれらの説明を省略する。加えて、前述のホスト計算機、バックアップサーバ及び前記ストレージサブシステム制御部及び設定端末には、それまでの処理を行うためプログラムや情報を格納するためのメモリ、CPU、内部のデータ通信路等の計算機において必ず存在する構成要素もそれぞれ存在するが、本発明の実施形態の説明においては重要でないため、ここではそれらの説明を省略する。

【0039】次に、t10 Technical CommitteeでSCSIのコマンドセットのドラフトとして開示されているInformation technology -SCSI Primary Command-3(SCP C3)に記載されている図を用いて、SCSI EXTENDED COPYコマンドのフォーマットについて、ロックデバイスからストリームデバイスへのコピー等を例として説明する。

【0040】図3はEXTENDED COPY CommandのCommand Descriptor Block(CDB)の構成を説明する図である。

【0041】EXTENDED COPY CommandのCDBは16バイトで構成され、バイト0に記載されている処理コード3100は83h(hは16進表示であることを示す)である。バイト1からバイト9までとバイト14とはリザーブ領域であり、バイト10からバイト13までにEXTENDED COPY Commandのパラメータリストの長さPARAMETER LIST LENGTH 3200が記載されている。

【0042】EXTENDED COPY Commandの実行に必要なパラメータは、CDBでの指定の他に、CDBに続いてホスト計算機からストレージサブシステムに対して、SC

SIにおけるイニシエータからターゲットに対してコマンドで指定したデータを送信するデータアウトフェーズにおいて、データアウトバッファに記載されて送信されてくる。

【0043】なお、前述のPARAMETER LIST LENGTH 3200の値が0である場合、何のデータも送信されなかつたことを示しており、エラーではない。

【0044】図4はEXTENDED COPY Command PARAMETER Listの構成を説明する図である。このリストは、図3で説明したように、CDBの処理コードが83hで、EXTENDED COPY Command であると判別された場合、データ・アウト・バッファ中に記載されているEXTENDED COPY Command の実行に必要なコマンドパラメータリストのフォーマットであり、図3に示すPARAMETER LIST LENGTH 3200は、このパラメータリストの長さをバイト値で示したものである。

【0045】EXTENDED COPY Command のパラメータリストは、16バイトからなるヘッダ部4700と、その後に続くターゲットディスクリプタ4500と、セグメントディスクリプタ4600と、オプションとしてのインラインデータとから構成される。ヘッダ部4700は、LIST IDENTIFIER4100、STR、NRCR、コマンドプライオリティ、ターゲットディスクリプタリストの長さ4200、セグメントディスクリプタリストの長さ4300、インラインデータの長さ4400の各データで構成される。

【0046】バイト0のLIST IDENTIFIER4100は、クライアントアプリケーションによって、SCSIのEXTENDED COPY Command をコピーマネージャに対してユニークに決めるために選ばれる値である。バイト1における7、6、3bit目はリザーブで、5bit目にはSTR、4bit目にはNRCR、2～0bit目にはPRIORITYが書き込まれている。

【0047】バイト2、3には、ターゲットディスクリプタ長4200であり、バイト16から記載されるターゲットディスクリプタ4500の長さが記載されており、バイト4～7はリザーブ、バイト8～11はセグメントディスクリプタ長(4300)で、バイトn+1から記載されるセグメントディスクリプタ4600の長さを記載している。なお、nはこのパラメータリスト中のターゲットディスクリプタが記載されている最後のバイト数である。

【0048】図5は図4に示したコマンドパラメータリスト内のバイト16からバイトnまでのターゲットディスクリプタ4500の内容の詳細を説明する図である。このターゲットディスクリプタは、1つ当たり32バイトで記述されていて、EXTENDED COPY Command のコピー元あるいはコピー先に関するデータを記述している。

【0049】図示ターゲットディスクリプタのバイト0には、ディスクリプタタイプコード5100が記述され

ていて、Fiber Channel World Wide Name のターゲットディスクリプタの場合、そのコードはE0hである。バイト1にはデバイスタイプ5200が記述されている。また、バイト4からバイト11までには、ターゲットのLogical Unit Number(LUN)5300が、バイト12から19までには、ターゲットのWorld Wide Name(WWN)5400が記述されている。さらに、バイト28からバイト31は、Device Type Specific Parameter 5500であり、ターゲットのデバイスタイプ固有のパラメータが記述されている。

【0050】図6は図5に示したターゲットディスクリプタのバイト28からバイト31に記述されているデバイス固有のパラメータ5500の詳細な内容の一例を説明する図であり、ターゲットディスクリプタにおいて、バイト1のbit4～0で指定したデバイスタイプがロックデバイス(例えば、ディスク)である場合のフォーマットである。

【0051】図7は図5に示したターゲットディスクリプタのバイト28からバイト31に記述されているデバイス固有のパラメータ5500の詳細な内容の他の例を説明する図であり、ターゲットディスクリプタにおいて、バイト1のbit4～0で指定したデバイスタイプがシーケンシャルアクセスデバイス(例えば、テープ)であった場合のフォーマットである。

【0052】図8は図4に示したコマンドパラメータリスト内のバイトn+1からバイトn+mまでに記述されているセグメントディスクリプタ4600の1つの詳細な内容の例を説明する図である。なお、mはパラメータリストにセグメントディスクリプタが記載されているデータ長である。

【0053】図示ターゲットディスクリプタのバイト0は、Descriptor Type Code8100であり、ここには、例えば、ロックデバイスからシーケンシャルアクセスデバイスへのコピーあるいはシーケンシャルアクセスデバイスからロックデバイスへのコピーであれば、00h、01h、0Bh、0Chの何れかのコードが記述される。バイト2、3には、ディスクリプタ長8200が記載されていてこのディスクリプタ長が記載されている後に続くセグメントディスクリプタの残り8800の長さを記述されている。前述のロックデバイスからテープデバイスへのコピーの場合、ここに記述されるコードは14hである。

【0054】バイト4、5には、コピー元となるソースターゲットディスクリプタインデックス8300が記述されており、バイト6、7には、コピー先のディスティネーションターゲットディスクリプタインデックス8400が記述される。これらのインデックスは、図4に記載のコマンドパラメータリスト内のターゲットディスクリプタ4500のインデックスと対応する。バイト9～11は、ストリームデバイス転送長8500であり、ス

トリークデバイスにデータを書き込む量を規定している。また、バイト14、15は、ブロックデバイスブロック数8600であり、図5のターゲットディスクリプタのフォーマット内に記述してある**DISK BLOCK LENGTH 6100**と対応する。バイト16～23に記述される**BLOCK DEVICELOGICAL BLOCK ADDRESS (LBA) 8700**は、Block Device上の最初の論理ブロックアドレスである。

【0055】前述で説明した図3～図8に示した**EXTENDED COPY Command**に関するフォーマットは、t10 Technical Committeeにおいて、SCSIのコマンドセットのドラフトとして開示されている。このため、前述したフォーマットの中身は今後変化する可能性はあるが、前述では、ターゲットのWWN、LUN等、コピー元コピー先を特定できる情報が前述のフォーマットに含まれていることを例示しただけであって、基本的に**EXTENDED COPY Command**の詳細部分の変更によって影響を受けることはない。

【0056】次に、**EXTENDED COPY Command**による不正なデバイスへのアクセスに対するアクセス制御に関して説明する。

【0057】前述した**EXTENDED COPY Command**は、ファイバチャネルの場合、ファイバチャネルフレームに納められ上位装置からストレージサブシステムに送信されてくる。そこで、まず、ファイバチャネルフレームについて説明する。

【0058】図9はファイバチャネルのフレームの構成を説明する図である。図示フレームは、フレームの始まりを示すSOF (start of frame) 9000と呼ばれる4バイトの識別子、リンク動作の制御やフレームの特徴づけを行う24バイトのフレームヘッダ9100、実際に転送される目的となるデータ部分であるデータフィールド9200、5バイトの巡回冗長コード (CRC) 9300、フレームの終わりを示すEOF (end of frame) 9400と呼ばれる4バイトの識別子からなる。データフィールドは、0～2112バイトの間で可変である。

【0059】図10は前述したファイバチャネルのフレーム内にあるフレームヘッダ部9100の構成を説明する図である。

【0060】フレームヘッダ部9100は、各ビットを持つ6つのWORDにより構成され、WORD0の23～0ビット領域は、D_ID (Destination ID) 10100、WORD1の23～0ビット領域は、S_ID (Source ID) 10200である。S_ID10200は、このファイバチャネルフレームを送信するポートを識別するための3バイトのアドレス識別子であり、D_ID10100は、このファイバチャネルフレームを受信するポートの識別を行う3バイトのアドレス識別子である。両識別子は、送受信される全てのフレームで有効な

値を持つ。S_ID10200は、上位装置（ホスト計算機やバックアップサーバ等）を動的に一意に識別できる情報であり、ファイバチャネルにおいてファイバチャネルフレームを送る送信元の機器と送信先の機器とがお互いに情報を交換し合うログイン時に上位装置より報告される値であり、デバイス間で論理セッションを確立するときには使用される。

【0061】前述したようなファイバチャネルフレームを使用することによって、ホスト計算機、バックアップサーバ等は、ストレージサブシステムとファイバチャネルを介してI/O処理を行うことが可能となる。

【0062】次に、本発明において、上位装置（ホスト計算機やバックアップサーバ）より、ファイバチャネルネットワークを介して**SCSI EXTENDED COPY**コマンドがあるファイバチャネルフレームを受信するためのストレージサブシステムが持つ情報テーブルの例について説明する。

【0063】図11は上位装置（例えば、ホスト計算機）からストレージサブシステムに送信されてくるファイバチャネルフレーム内のS_IDとそれに対応する上位装置のWWNとの対応付けを行うテーブルの例を説明する図である。

【0064】図示テーブルは、ホスト計算機がストレージサブシステムにファイバチャネルを介しログインを行う際に、ファイバチャネルフレームからホスト計算機（ホスト計算機バスアダプタのポート）のWWNとS_IDとを取得する等によって作成される。

【0065】ログイン後、通常のファイバチャネルは、S_ID、D_IDを使用して通信を行う。図11に示すテーブルの1列目11100はS_IDであり、2列目11200はそれに対応したホスト計算機のWWNである。

【0066】ファイバチャネルフレームを受信したストレージサブシステムは、ファイバチャネルフレーム内のS_IDを取り出し、図示テーブルの1列目を検索を行ってマッチしたS_IDに対応するWWNを取得することができる。これにより、そのファイバチャネルフレームを送信してきたホスト計算機のWWNを特定することができる。

【0067】なお、ファイバチャネルのログイン処理は、本発明に直接関係ないので、ここでの説明は省略する。

【0068】すなわち、ホスト計算機がファイバチャネルログイン後ストレージサブシステムの論理デバイスに対して、**EXTENDED COPY Command**を送信してくると、そのコマンドを受領する論理デバイスを制御するストレージサブシステム制御部2200は、ファイバチャネルフレームヘッダからS_IDを取り出し、図11に示すテーブルを参照し、そのS_IDに対応するフレームを送信してきたホスト計算機のWWNを割り出すことができる。

るる。

【0069】図12は図2に示したLUN～WWNアクセス可否情報2221の例を説明する図であり、ホスト計算機のWWN12100と、ストレージサブシステムのあるポート（ポートのWWN：1234567890ABCDEF）12000のポート毎に関連付けられたLUN12000において、あるWWNを持つホスト計算機がどのLUNにアクセスできるかという対応関係を示した例をテーブルとして図示したものである。

【0070】説明している本発明の実施形態の場合、図12に示すテーブルは、ストレージサブシステム上にあるポート毎に作成され、ストレージサブシステムに存在するポート数分の複数が存在する。そして、テーブルの作成は、ストレージサブシステムと通信可能な保守用の装置、例えば、設定端末2700から、入力手段とその入力結果を確認するための表示手段とを用いて指示することにより行われる。

【0071】設定手段としては、ストレージサブシステムにLANや電話回線または内部バスによって接続されているストレージサブシステムの保守用設定端末から行われるのが一般的であるが、本発明は、それらを設定する設定者の場所やそれらの設定手段、設定端末の種類、使用するネットワークの種類等は特に問わない。また、ここで用いられているWWNは既知であるとする。

【0072】通信回線の種類により、LANを用いればストレージサブシステムに近い場所からの設定、電話回線を用いれば保守センタ等遠隔地からの設定が可能である。また、内部バスを用いて保守用装置とストレージサブシステムとを一体化させることも可能である。

【0073】LUNは、ポートに関連付けられたLUを示し、WWNの数は、そのポート配下に存在するLUへアクセスする可能性のあるホスト計算機の数だけ存在する。LU及びホスト計算機の数は有限な数となる。

【0074】テーブルの各要素において、本発明の実施形態では、値“1”がアクセス許可を、値“0”がアクセス拒否を意味することにする。

【0075】図12に示す例の場合、そのポートにおいて、LUN0（12210）へアクセス許可があるホスト計算機は、WWNが“0123456789ABCDEF”及び“0123456789ABCDEF”を持つホスト計算機であり、LUN1（12220）へアクセス許可があるホスト計算機は、WWNが“0123456789ABCDEF”を持つホスト計算機である。また、図示例の場合、LUNn-1（12230）へのアクセスが許可されているホスト計算機は、存在しないことを表している。

【0076】さて、ホスト計算機が、EXTENDED COPY Commandをストレージサブシステムの論理デバイスに対して発行すると、ストレージサブシステムは、このコマンドを受信した際に、ホスト計算機のWWNとコマンドの

送信先である論理デバイスの識別子LUNとをチェックし、アクセス可能か否かを評価した後、論理デバイスがこのコマンドを受領してコマンドの内容を解析し始める。受領したコマンドがEXTENDED COPY Commandである場合、EXTENDED COPY処理手段2230は、そのコマンド受領論理デバイスがコピーマネージャとなり、コマンド内に記載されたコピー元の論理デバイスからコピー先の論理デバイスに対してデータのコピーを行うように制御する。

【0077】図13はLUN～WWNアクセス可否情報更新の処理動作の例を説明するフローチャートであり、次に、これについて説明する。ここで説明する例は、図11により説明した上位装置（例えば、ホスト計算機）からストレージサブシステムに送信されてくるファイバチャネルフレーム内のS_IDとそれに対応する上位装置のWWNの対応付けを行うテーブルと、図12により説明した図2のLUN～WWNアクセス可否情報2221の例で、ホスト計算機のWWNとストレージサブシステムのあるポート毎に関連付けられたLUNにおいて、あるWWNを持つホスト計算機がどのLUNにアクセス（ポートログイン等）ができるかの対応関係を示したテーブルとの設定に関するストレージサブシステム制御部の処理手順の一例である。なお、ここでは、予め設定されている論理デバイス以外に新たに論理デバイスを設定する場合を例にあげて説明する。

【0078】（1）まず、例えば、ホスト計算機やバックアップサーバは、READ/ WRITEを行う論理ボリュームのある時点のレプリケーション（静的なイメージ）用のデバイスとして、または、ディザスタリカバリ

等の用途で、ホストのI/O処理を行うボリュームとは物理的に遠隔でネットワークで接続されたボリュームに、遠隔地へのコピー先用途等で、新たに論理デバイスを指定した空き物理記憶領域から割当るように、I/Oネットワーク2600やネットワーク2500を用い指示する。あるいは、ストレージサブシステム管理者が設定端末2700を使用して、ホスト計算機ユーザからの要求に対応して、新たに論理デバイスを指定した空き物理記憶領域から割当るように指示する。ストレージサブシステム制御部2200は、その要求を受領して、指定の空き物理記憶領域から論理デバイスを割当て、論理/物理対応手段2211を用いて、論理/物理対応情報2212を更新する（ステップ13100、13200）。

【0079】（2）次に、ストレージサブシステム制御部2200は、割り当てた論理デバイスに対して、図12により説明したLUN～WWNアクセス可否情報2221を更新する。この更新は、例えば、新規に割り当てた論理デバイスに対しては、指示を出したバックアップサーバのWWNとバックアップを行なうデータを正ボリューム側でI/O処理を行うHOST計算機のWWNと

を許可する、というように行われる（ステップ13300）。

【0080】前述したLUN～WWNアクセス可否情報2221の更新は、ストレージサブシステム管理者が設定端末を使用して設定してもよいし、例えば、ストレージサブシステム制御部内のコマンド処理部2213がLUN SECURITY設定処理をプログラム処理して行ってもよい。

【0081】図14はファイバチャネルネットワークを介してSCSI EXTENDED COPYコマンドを受領したデバイスでの処理動作の例を説明するフローチャートであり、次に、これについて説明する。ここで説明する例は、上位装置からファイバチャネルネットワークを介してSCSI EXTENDED COPYコマンドが送信されてきた場合に、ファイバチャネルフレームを受信したストレージサブシステム制御部2200と、EXTENDED COPYアクセス制御手段2230と、EXTENDED COPYアクセス制御手段2231によって受領論理デバイスが行う処理の例である。

【0082】また、ここでは、EXTENDED COPY Commandは、図9に示すFCP_CMNDと呼ばれる情報単位を含むフレームとして、ファイバチャネルネットワークを介してホスト計算機からストレージサブシステムへ送信された場合について述べる。

【0083】（1）図2に示すようなホスト計算機からのファイバチャネルフレームを受信するストレージサブシステムは、まず、ファイバチャネルログインの処理において、フレームからS_ID、及びWWNを取り出し、そのファイバチャネルフレーム送信元のホスト計算機のS_IDと図11に示すようなWWNの対応テーブルを作成し、また、当該ホスト計算機がストレージサブシステム内の指定デバイスに対してアクセス可能か否かを図12に示すテーブルを用いてチェックする。その後、ストレージサブシステムは、内部の特定論理デバイスに対して前述のホスト計算機より送信されてくるファイバチャネルフレームを受信する（ステップ14000）。

【0084】（2）ファイバチャネルフレームを受信すると、このフレームを送信してきたホスト計算機のWWNを識別できるようにフレームヘッダ内のS_IDを取り出す。次に、フレームのデータフィールドを読み、ファイバチャネルフレーム内にCommand Device Block (CDB) があった場合で、コマンドの内容がEXTENDED COPY Commandであるか否かを評価する（ステップ14010、14020）。

【0085】（3）ステップ14020の評価で、受信したファイバチャネルフレームがEXTENDED COPY Commandではなかった場合、他の処理に移行する（ステップ14031）。

【0086】（4）ステップ14020の評価で、受信したファイバチャネルフレームがEXTENDED COPY Command

dであった場合、次に、CDB内のパラメータ長の評価を行い、パラメータ長が0であれば、処理を終了し、パラメータ長が0でなければ、CDBに続く、図4示したコマンドパラメータリストの読み込みを開始する（ステップ14030）。

【0087】（5）コマンドパラメータリスト内のリストID等を読み込んだ後、バイト2、3のターゲットディスクリプタ長の読み込みを行う。ここでは、ターゲットディスクリプタ長が、例えば、TLであったとする（ステップ14040）。

【0088】（6）次に、バイト8～11のセグメントディスクリプタ長の読み込みを行う。ここでは、セグメントディスクリプタ長が、例えば、SLであったとする（ステップ14050）。

【0089】（7）パラメータリストのオンラインデータ長を読み込んだ後、ターゲットディスクリプタを1ターゲットディスクリプタ長分（32Byte）づつ読み込んでいく。なお、このEXTENDED COPY Commandに含まれるターゲットディスクリプタの数は、TL/32である。ターゲットディスクリプタのフォーマットは図5によりすでに説明しており、まず、ディスクリプタのタイプコードを評価し、ターゲットのWWN及びLUNを読み込む。前述の1ターゲットディスクリプタの読み込みの処理を、ターゲットディスクリプタ個数分（TL/32個）繰り返す（ステップ14060～14100）。

【0090】（8）次に、セグメントディスクリプタの読み込みを行う。セグメントディスクリプタのフォーマットは図8によりすでに説明しており、まず、ディスクリプタタイプコード、ディスクリプタ長（DL）等を読み込む。次に、コピー元論理デバイスとなるソースターゲットのディスクリプタインデックス、コピー先論理デバイスとなるディスティネーションターゲットのディスクリプタインデックスを読み込む（ステップ14120～14150）。

【0091】（9）ここで、セグメントディスクリプタに記述されているターゲットディスクリプタインデックスをキーとして、図5に示すターゲットディスクリプタを参照し、ソースターゲットのWWN、LUNを読み込んで、図12に示すホスト計算機WWNと論理デバイス（LU）とのアクセス可否のテーブルを参照し、ソースターゲットのWWN及びLUNとこのEXTENDED COPY Commandを送信したWWNのホスト計算機がソースターゲットに指定された論理デバイスに対してアクセス可能か否かの評価を行う（ステップ14160、14170）。

【0092】（10）ステップ14170での評価で、アクセス可能であった場合、セグメントディスクリプタの残りを読み込んで、転送長やブロックデバイス数、ブロックデバイスのLBAなどを読み込み、指定されたデータコピーを、ソースターゲットで指定された論理デバイ

スからディスティネーションターゲットに指定された論理デバイスに向けてコピーを行う（ステップ14180）。

【0093】（11）そして、次のセグメントディスクリプタを読み込むステップ14120からの処理を繰り返す。これを、前記ディスクリプタ長（DL）とセグメントディスクリプタ長（SL）とから求まる、SL/（DL+4）回繰り返す（ステップ14110～14190）。

【0094】（12）ステップ14170での評価で、ソースターゲットに指定された論理デバイスに対してアクセス拒否あるいは不可能であった場合、このEXTENDED COPY CommandをCHECK CONDITION statusで終了し、例えば、sense keyにCOPY ABORTを設定し、sense codeにCOPY TARGET DEVICE NOT REACHABLEを設定し、これに対応した例外処理として、EXTENDED COPY Commandで定められた適切なエラー処理を行い、エラーをホストに通知して処理を終了する（ステップ14210、14200）。

【0095】なお、前述では、アクセス可否の個所のみにエラー処理を行うとして説明したが、コマンド自体のエラー処理は、その時々のステップ毎においてEXTENDED COPY Commandで定められたものがあり、当然エラーが発生した際はそれに従う。

【0096】（13）また、ステップ14190で全セグメントディスクリプタ分の前述した処理が終了したことが確認できれば、インラインデータ長が0のとき、EXTENDED COPY Command処理をEXTENDED COPY Commandで定められた正常終了処理を行って、EXTENDED COPY Commandの処理を終了する（ステップ14200）。

【0097】図15はファイバチャネルネットワークを介してSCSI EXTENDED COPYコマンドを受領したデバイスでの処理動作の他の例を説明するフローチャートであり、次に、これについて説明する。ここで説明する例は、上位装置からファイバチャネルネットワークを介してSCSI EXTENDED COPYコマンドが送信された場合に、ファイバチャネルフレームを受信したストレージサブシステム制御部2200と、EXTENDED COPYアクセス処理手段2230と、EXTENDED COPYアクセス制御手段2231とによって受領論理デバイスが行う処理の例であり、図14に示すフローで制御したものに対して、ディスティネーションターゲットディスクリプタに記載のWWN、LUNをもLUNアクセステーブルでアクセス可否テーブルを用いて評価する処理（ステップ15170～15190）が加えてある。この加えられた処理は、ストレージサブシステム内部の、レプリケーションや遠隔コピー用のために予め処理を予約されている論理ボリュームに対して、コピー先に指定してEXTENDED COPYのコピー処理を行うことができないようにする等のために利用することができる。

【0098】ここでは、EXTENDED COPY Commandは、図9に示すFCP_CMNDと呼ばれる情報単位を含むフレームとして、ファイバチャネルネットワークを介してホスト計算機からストレージサブシステムへ送信された場合について制御する。

【0099】（1）図2に示すようなホスト計算機からのファイバチャネルフレームを受信するストレージサブシステムは、まず、ファイバチャネルログインの処理において、フレームからS_ID、及びWWNを取り出し、そのtファイバチャネルフレーム送信元のホスト計算機のS_IDと図11に示すようなWWNの対応テーブルを作成し、また、当該ホスト計算機がストレージサブシステム内の指定デバイスに対してアクセス可能か否かを図12に示すテーブルを用いてチェックする。その後、ストレージサブシステムは、内部の特定論理デバイスに対して前述のホスト計算機より送信されてくるファイバチャネルフレームを受信する（ステップ15000）。

【0100】（2）ファイバチャネルフレームを受信すると、このフレームを送信してきたホスト計算機のWWNを識別できるようにフレームヘッダ内のS_IDを取り出す。次に、フレームのデータフィールドを読み、ファイバチャネルフレーム内にCommand Device Block (CDB) があった場合で、コマンドの内容がEXTENDED COPY Commandであるか否かを評価する（ステップ15010、15020）。

【0101】（3）ステップ15020の評価で、受信したファイバチャネルフレームがEXTENDED COPY Commandではなかった場合、他の処理に移行する（ステップ15031）。

【0102】（4）ステップ15020の評価で、受信したファイバチャネルフレームがEXTENDED COPY Commandであった場合、次に、CDB内のパラメータ長の評価を行い、パラメータ長が0であれば、処理を終了し、パラメータ長が0でなければ、CDBに続く、図4示したコマンドパラメータリストの読み込みを開始する（ステップ15030）。

【0103】（5）コマンドパラメータリスト内のリストID等を読み込んだ後、バイト2、3のターゲットディスクリプタ長の読み込みを行う。ここでは、ターゲットディスクリプタ長が、例えば、TLであったとする（ステップ15040）。

【0104】（6）次に、バイト8～11のセグメントディスクリプタ長の読み込みを行う。ここでは、セグメントディスクリプタ長が、例えば、SLであったとする（ステップ15050）。

【0105】（7）パラメータリストのインラインデータ長を読み込んだ後、ターゲットディスクリプタを1ターゲットディスクリプタ長分（32Byte）づつ読み込んでいく。なお、このEXTENDED COPY Commandに含ま

れるターゲットディスクリプタの数は、TL/32である。ターゲットディスクリプタのフォーマットは図5によりすでに説明しており、まず、ディスクリプタのタイプコードを評価し、ターゲットのWWN及びLUNを読み込む。前述の1ターゲットディスクリプタの読み込みの処理を、ターゲットディスクリプタ個数分(TL/32個)繰り返す(ステップ15060~15100)。

【0106】(8) 次に、セグメントディスクリプタの読み込みを行う。セグメントディスクリプタのフォーマットは図8によりすでに説明しており、まず、ディスクリプタタイプコード、ディスクリプタ長(DL)等を読み込む。次に、コピー元論理デバイスとなるソースターゲットのディスクリプタインデックス、コピー先論理デバイスとなるディスティネーションターゲットのディスクリプタインデックスを読み込む(ステップ15120~15150)。

【0107】(9) ここで、セグメントディスクリプタに記述されているターゲットディスクリプタインデックスをキーとして、図5に示すターゲットディスクリプタを参照し、ソースターゲットのWWN、LUNを読み込んで、図12に示すホスト計算機WWNと論理デバイス(LU)とのアクセス可否のテーブルを参照し、ソースターゲットのWWN及びLUNとこのEXTENDED COPY Commandを送信したWWNのホスト計算機がソースターゲットに指定された論理デバイスに対してアクセス可能か否かの評価を行う(ステップ15160、15170)。

【0108】(10) ステップ15170での評価で、アクセス可能であった場合、次に、コピー先の論理デバイスとなるディスティネーションターゲットのディスクリプタインデックスを読み込んでターゲットディスクリプタを参照する(ステップ15180)。

【0109】(11) ここで、セグメントディスクリプタに記述されているターゲットディスクリプタインデックスをキーとして、図5に示すターゲットディスクリプタを参照し、ディスティネーションターゲットのWWN、LUNを読み込んで、図12に示すホスト計算機WWNと論理デバイス(LU)とのアクセス可否のテーブルを参照し、ディスティネーションターゲットのWWN及びLUNとこのEXTENDED COPY Commandを送信したWWNのホスト計算機がソースターゲットに指定された論理デバイスに対してアクセス可能か否かの評価を行う(ステップ15190、15200)。

【0110】(12) ステップ15200での評価で、アクセス可能であった場合、セグメントディスクリプタの残りを読み込んで、転送長やブロックデバイス数、ブロックデバイスのLBAなどを読み込み、指定されたデータコピーを、ソースターゲットで指定された論理デバイスからディスティネーションターゲットに指定された論理デバイスに向けてコピーを行う(ステップ1521

0)。

【0111】(13) そして、次のセグメントディスクリプタを読み込むステップ15120からの処理を繰り返す。これを、前記ディスクリプタ長(DL)とセグメントディスクリプタ長(SL)とから求まる、SL/(DL+4)回繰り返す(ステップ15110~1520)。

【0112】(14) ステップ15170、15200での評価で、ソースターゲット、あるいは、ディスティネーションターゲットに指定された論理デバイスに対してアクセス拒否あるいは不可能であった場合、このEXTENDED COPY CommandをCHECK CONDITION statusで終了し、例えば、sense keyにCOPY ABORTを設定し、sense codeにCOPY TARGET DEVICE NOT REACHABLEを設定し、これに対応した例外処理として、EXTENDED COPY Commandで定められた適切なエラー処理を行い、エラーをホストに通知して処理を終了する(ステップ15230、15240)。

【0113】なお、前述では、アクセス可否の個所のみにエラー処理を行うとして説明したが、コマンド自体のエラー処理は、その時々のステップ毎においてEXTENDED COPY Commandで定められたものがあり、当然エラーが発生した際はそれに従う。

【0114】(15) また、ステップ15220で全セグメントディスクリプタ分の前述した処理が終了したことが確認できれば、インラインデータ長が0のとき、EXTENDED COPY Command処理をEXTENDED COPY Commandで定められた正常終了処理を行って、EXTENDED COPY Commandの処理を終了する(ステップ15240)。

【0115】前述した本発明の実施形態によれば、上位装置の識別子及び情報を記憶するデバイスとの間のアクセス可否情報と、その情報保持及びその情報を用いたアクセス可否判定手段と、ストレージサブシステム内部からの能動的なコピー指示コマンドによるコピー処理実行時にコピー実行の可否を判断する手段とを備えることにより、ホスト計算機等の上位装置からストレージサブシステム内の論理デバイスに対するアクセス可否を、上位装置のWWNと論理デバイス識別子LUとの対応関係によりチェックを行うことに加えて、上位装置からストレージサブシステムに対して発行されるストレージサブシステム内部からの能動的なコピー指示コマンドを処理する際に、コピー指示デバイスとなるコピー受領論理デバイスが、コピー元デバイスとコピー先デバイス各々に対してアクセス制御を行うチェックを実行することによって判定し、ストレージサブシステム内部からの能動的なコピー指示コマンドによる不正なデータの流出を防止することができる。

【0116】

【発明の効果】以上説明したように本発明によれば、SCI EXTENDED COPYコマンド等の制御コマンドによるスト

レージサブシステムからのデータコピーに対し、コピー元ボリュームでのWWNレベルでのセキュリティチェックを実現し、複数の上位装置からストレージサブシステム及びストレージサブシステム内の記憶領域へのアクセスを選択的に制限することを可能として、不正なデータコピーを防止することができる。

【図面の簡単な説明】

【図1】従来技術の問題点について説明するストレージサブシステムとホスト計算機との関係を示す図である。

【図2】本発明の一実施形態によるストレージサブシステムを用いた計算機システムの構成を示すブロック図である。

【図3】EXTENDED COPY CommandのCommand Descriptor Block(CDB)の構成を説明する図である。

【図4】EXTENDED COPY Command PARAMETER Listの構成を説明する図である。

【図5】図4に示したコマンドパラメータリスト内のバイト16からバイトnまでのターゲットディスクリプタ4500の内容の詳細を説明する図である。

【図6】図5に示したターゲットディスクリプタのバイト28からバイト31に記述されているデバイス固有のパラメータの詳細な内容の一例を説明する図である。

【図7】図5に示したターゲットディスクリプタのバイト28からバイト31に記述されているデバイス固有のパラメータの詳細な内容の他の例を説明する図である。

【図8】図4に示したコマンドパラメータリスト内のバイトn+1からバイトn+mまでに記述されているセグメントディスクリプタの詳細な内容の例を説明する図である。

【図9】ファイバチャネルのフレームの構成を説明する図である。

【図10】前述したファイバチャネルのフレーム内にあるフレームヘッダ部の構成を説明する図である。

【図11】上位装置からストレージサブシステムに送信

されてくるファイバチャネルフレーム内のS_IDとそれに対応する上位装置のWWNとの対応付けを行うテーブルの例を説明する図である。

【図12】図2に示したLUN～WWNアクセス可否情報の例を説明する図である。

【図13】LUN～WWNアクセス可否情報更新の処理動作の例を説明するフローチャートである。

【図14】ファイバチャネルネットワークを介してSCSI EXTENDED COPYコマンドを受領したデバイスでの処理動作の例を説明するフローチャートである。

【図15】ファイバチャネルネットワークを介してSCSI EXTENDED COPYコマンドを受領したデバイスでの処理動作の他の例を説明するフローチャートである。

【符号の説明】

2000、2001 ホスト計算機

2002 バックアップサーバ

2100 ストレージサブシステム

2200 ストレージサブシステム制御部

2210 リード／ライト処理手段

2211、2212 論理／物理対応情報

2213 コマンド処理部

2214 SCSIコマンド処理部

2220 LUNセキュリティアクセス制御手段

2221 LUN～WWNアクセス可否情報

2222 WWN～S_ID対応情報

2230 EXTENDED COPY 処理手段

2231 EXTENDED COPY アクセス制御手段

2240 外部装置通信処理部

2300 物理記憶装置

2401～2412、2420 論理デバイス

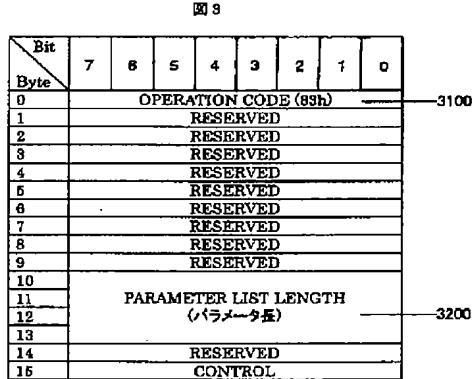
2500 ネットワーク

2600 I/Oネットワーク

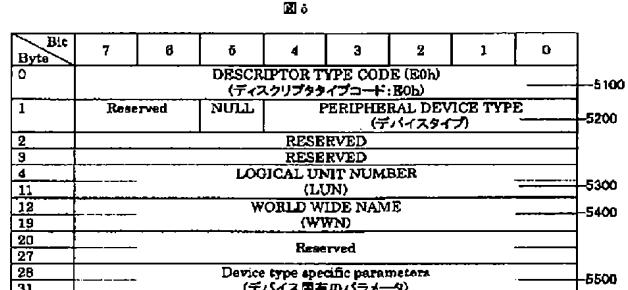
2610 I/Oバス

2700 設定端末

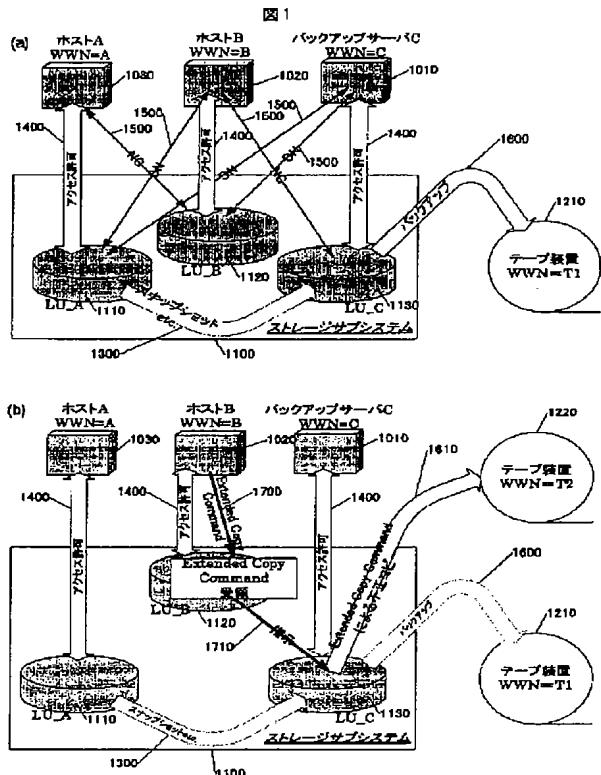
【図3】



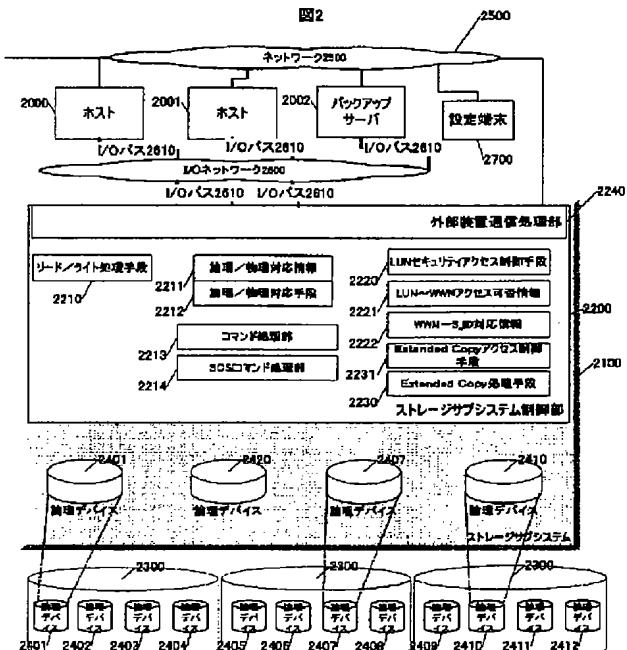
【図5】



【図1】



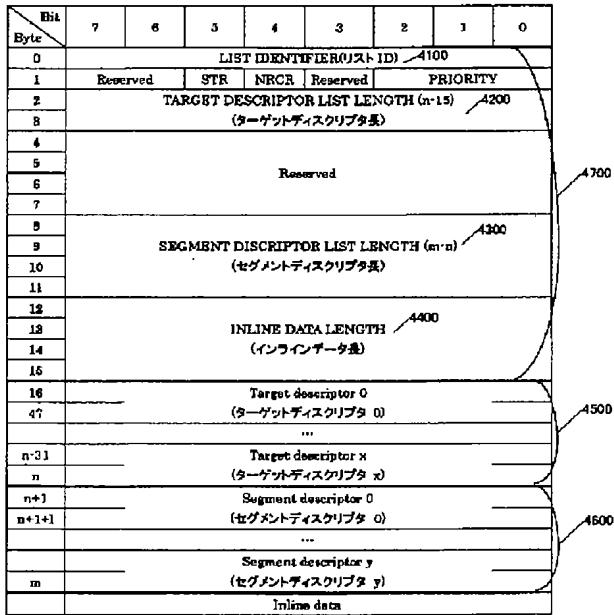
【図2】



【図6】

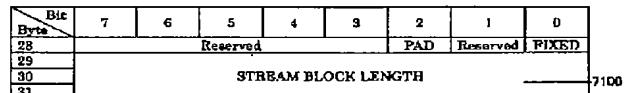
【図4】

4

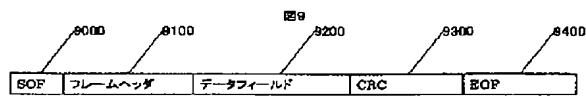


[图 3]

四 7



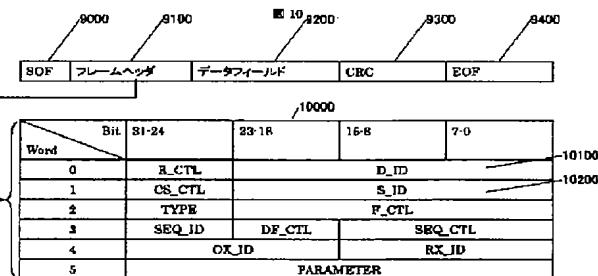
【図9】



【図 8】

Bit Byte	7	6	5	4	3	2	1	0	
0	DESCRIPTOR TYPE CODE (00h, 01h, 09h, or 0Ch)								8100
1	Reserved								CAT
2	DESCRIPTOR LENGTH 0014h 8200								
3	(ディスクリプタ長)								
4	SOURCE TARGET DESCRIPTOR INDEX 8800 (ソース - ターゲット ディスクリプタ インデックス)								
5	DESTINATION TARGET DESCRIPTOR INDEX 8400 (ディスティネーション ターゲット ディスクリプタ インデックス)								
6	Reserved								
7	STREAM DEVICE TRANSFER LENGTH 8500 (ストリームデバイス転送長[Byte])								8800
8	Reserved								
9	BLOCK DEVICE NUMBER OF BLOCKS 8800 (ブロックデバイスブロック数)								
10	BLOCK DEVICE LOGICAL BLOCK ADDRESS 8700 (LBA)								
11	Reserved								
12	Reserved								
13	Reserved								
14	BLOCK DEVICE NUMBER OF BLOCKS 8800 (ブロックデバイスブロック数)								
15	BLOCK DEVICE LOGICAL BLOCK ADDRESS 8700 (LBA)								
16	BLOCK DEVICE LOGICAL BLOCK ADDRESS 8700 (LBA)								
29	BLOCK DEVICE LOGICAL BLOCK ADDRESS 8700 (LBA)								

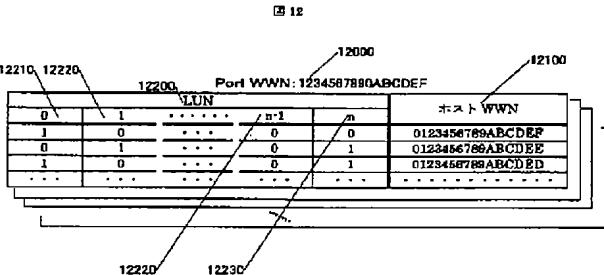
【図 10】



【図 11】

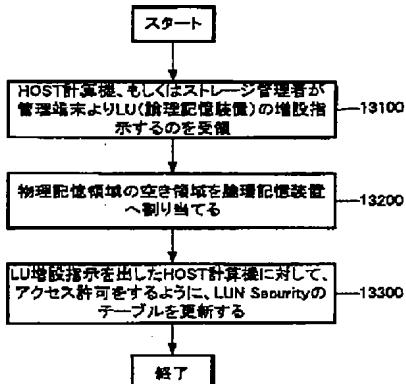
11100	1111	11200
S_ID	ホスト WWN	
FFFF01	0123456789ABCDEF	
FFFF02	0123456789ABCDEF	
FFFF03	0123456789ABCDEF	
...	...	

【図 12】

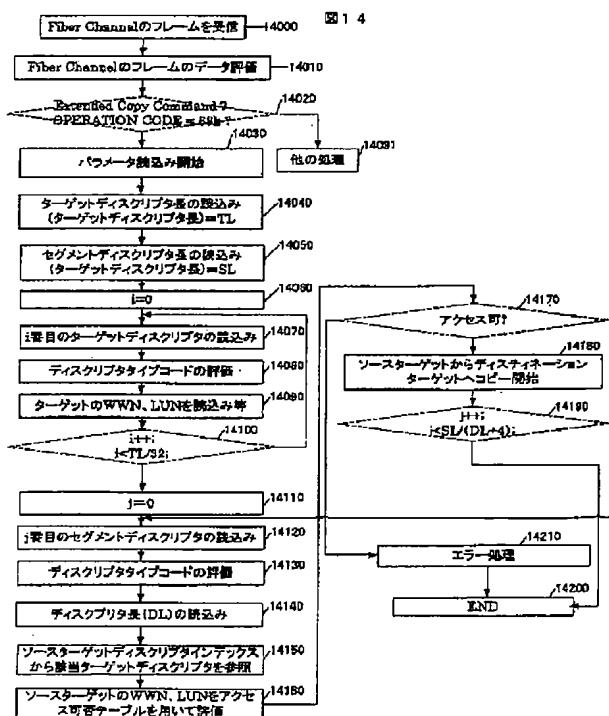


【図 13】

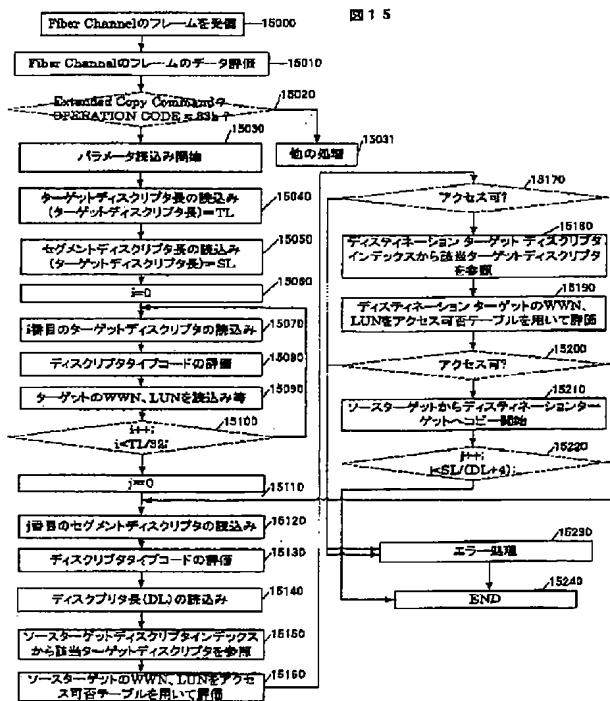
図 13



【図 14】



【図15】



フロントページの続き

(72) 発明者 藤田 高広
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内
(72) 発明者 田村 圭史
神奈川県小田原市国府津2880番地 株式会社日立製作所ストレージ事業部内

(72) 発明者 岡見 ▲吉▼規
神奈川県小田原市国府津2880番地 株式会社日立製作所ストレージ事業部内
F ターム(参考) 5B017 AA03 BA06 BB06 CA07 CA16
5B065 BA01 PA04 PA12
5B082 DE03 EA11